

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

SECURITY PLANNING FOR WIRELESS NETWORKS: DOD CONCERNS

by

James D. Fowler

March 1999

Thesis Advisor:
Associate Advisor:

Cynthia E. Irvine
Douglas Brinkley

19990512 031

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 1999		3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE : Security Planning for Wireless Networks: DoD Concerns			5. FUNDING NUMBERS	
6. AUTHOR(S) Fowler, James D.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (<i>maximum 200 words</i>) Wireless networking is a rapidly emerging technology and security must be addressed as it is incorporated into new and existing local area networks (LANs). It is important to know what unique properties of wireless LANs might amplify existing LAN vulnerabilities or introduce new ones. Wireless transmission techniques, topologies, and vendor offerings were surveyed from a security perspective. Three rating systems were developed to analyze aspects of these survey areas. These areas were then rated using these systems and graphically displayed on Kiviat drawings to show symmetric comparisons of each analysis category. Frequency hopping spread spectrum (FHSS) transmission technology, cellular topology, and the Jaguar product emerge as the best current approaches available. These results are applied to a case study that examines network wired segment replacement options, wireless segment attacks, and methods to detect an attacker. Current standards offer guidance that dictate how wireless technologies must operate, but do not relate to principles of LAN design. Our study and rating system results provide guidance for creating a network topology. The case study demonstrated that care must be taken in choosing wireless network segments. This work should help System Administrators by providing examples of good and bad choices.				
14. SUBJECT TERMS Security, Local/Wide Area Networks (LANs), Intranetworks			15. NUMBER OF PAGES 99	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

Approved for public release; distribution is unlimited

SECURITY PLANNING FOR WIRELESS NETWORKS: DOD CONCERNS

James D. Fowler
Lieutenant, United States Navy
B.A., University of Oklahoma, 1990

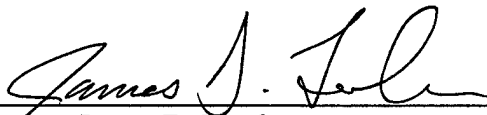
Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

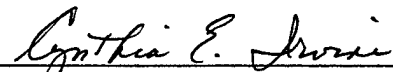
from the

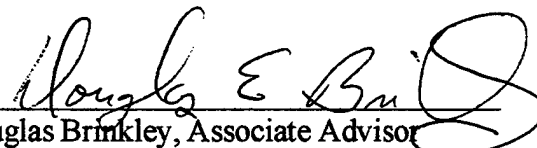
**NAVAL POSTGRADUATE SCHOOL
March 1999**

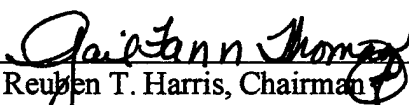
Author:


James D. Fowler

Approved by:


Cynthia E. Irvine, Thesis Advisor


Douglas Brinkley, Associate Advisor


Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

Wireless networking is a rapidly emerging technology and security must be addressed as it is incorporated into new and existing local area networks (LANs). It is important to know what unique properties of wireless LANs might amplify existing LAN vulnerabilities or introduce new ones.

Wireless transmission techniques, topologies, and vendor offerings were surveyed from a security perspective. Three rating systems were developed to analyze aspects of these survey areas. These areas were then rated using these systems and graphically displayed on Kiviat drawings to show symmetric comparisons of each analysis category.

Frequency hopping spread spectrum (FHSS) transmission technology, cellular topology, and the Jaguar product emerge as the best current approaches available. These results are applied to a case study that examines network wired segment replacement options, wireless segment attacks, and methods to detect an attacker. Current standards offer guidance that dictate how wireless technologies must operate, but do not relate to principles of LAN design. Our study and rating system results provide guidance for creating a network topology. The case study demonstrated that care must be taken in choosing wireless network segments. This work should help System Administrators by providing examples of good and bad choices.

TABLE OF CONTENTS

I. INTRODUCTION	1
A. WIRELESS LOCAL AREA NETWORKS.....	1
1. Advantages of wireless over wired	1
2. Department of Defense Applications	2
B. PROBLEM STATEMENT	2
C. THESIS OVERVIEW	2
II. BACKGROUND	5
A. TECHNOLOGY OVERVIEW: WIRELESS TRANSMISSION TECHNIQUES.....	5
1. Narrowband Microwave	5
2. Infrared	6
3. Spread Spectrum	7
B. TECHNOLOGY OVERVIEW: WIRELESS TOPOLOGIES	10
1. Ad Hoc	13
2. Cellular	14
3. Non-Cellular	15
4. Personal Area Networks	16
C. TECHNOLOGY OVERVIEW: VENDORS.....	16
1. Air-I/O.....	16
2. Jaguar	18
3. WaveLyNX BR 132™	20
4. NetWeaver	21
III. SECURITY CONCERNS FOR WIRELESS.....	25
A. GENERAL SECURITY LEVELS	25
1. Secure Military Systems	25
2. Secure Public Systems.....	26
B. LOGICAL ACCESS.....	28
C. ATTACKS: LAN VERSUS WLAN.....	28
1. Eavesdropping	29
2. Transitive Trust.....	30
3. Infrastructure.....	30
4. Physical Denial of Service.....	30
D. ANALYSIS OF TOOLS WITHIN THE WIRELESS CONTEXT.....	31
1. Hacker Tools in WLANs	31
2. Intrusion detection tools	34
E. SECURITY STANDARDS.....	36
1. HIPERLAN	36
2. IEEE 802.11.....	37
F. CONCLUSION	39
IV. ANALYSIS AND EVALUATION	41

A. TRANSMISSION TECHNOLOGIES	42
1. Transmission Technology Evaluation	43
2. Best Technology Analysis	47
B. TOPOLOGIES	48
1. Topology Evaluation.....	48
2. Best Topology Analysis	51
C. VENDOR TOPOLOGIES.....	51
1. Vendor Topology Evaluation.....	51
2. Best Vendor Topology Analysis	55
D. WLAN CASE STUDY: WIRED SEGMENT REPLACEMENT	55
1. Wireless Between User and Multistation Access Unit	58
2. Wireless Between Servers and Multistation Access Units	60
3. Wireless Between Multistation Access Units	62
4. Wireless Between Backbone and Ingersoll LAN	64
5. Summary	65
E. WIRELESS LAN CASE STUDY: WIRELESS SEGMENT ATTACKS	66
1. By-passing Access Controls; Frequency Hopping Algorithm Known.....	66
2. Bypassing the Firewall; Frequency Hopping Algorithm Known	68
3. Direct Connection to Wireless Users; Frequency Hopping Algorithm Known.....	69
4. IP Spoofing Between Multistation Access Units; Frequency Hopping Algorithm Known.....	71
5. Denial of Service; Frequency Hopping Algorithm Not Known	72
F. WIRELESS LAN CASE STUDY: DETECTING THE ATTACKER	73
1. Software Sniffers	74
2. Hardware Detector Detectors	74
V. CONCLUSION	77
APPENDIX A. ABBREVIATIONS	79
APPENDIX B. DEFINITIONS.....	81
APPENDIX C. OSI MODEL LAYERS.....	83
INITIAL DISTRIBUTION LIST	85

LIST OF FIGURES

Figure 1: A Wireless Peer-to-Peer Network	10
Figure 2: Client and Access Point	11
Figure 3: Multiple Access Points and Roaming	11
Figure 4: Extension Point Providing Coverage Between APs and Mobile Users.....	12
Figure 5: The Use Of Directional Antennas	12
Figure 6: Ad Hoc Without Centralized Control.....	13
Figure 7: Ad Hoc With Centralized Control	14
Figure 8: Cellular	15
Figure 9: Non-Cellular	15
Figure 10: Personal Area Networks	16
Figure 11: Air-I/O	17
Figure 12: Jaguar's 3.2 Mbps Wireless LAN	19
Figure 13: Jaguar Access Point Configuration	20
Figure 14: WaveLyNX BR 132.....	21
Figure 15: NetWeaver	22
Figure 16: NetWeaver CU Topology	23
Figure 17: Electronic Warfare Overview for Military Systems.....	26
Figure 18: Wireless Public Information Network.....	27
Figure 19: HIPERLAN Encryption-Decryption Scheme	37
Figure 20: WEP Mechanism	39
Figure 21: Shaded Kiviat Diagram	42
Figure 22: Technology Evaluation.....	47
Figure 23: Best Technology (FHSS)	47
Figure 24: Topology Evaluation	50
Figure 25: Best Topology (Cellular).....	51
Figure 26: Vendor Topology Evaluation	54
Figure 27: Best Vendor Topology (Jaguar)	54
Figure 28: Ingersoll 224 Token Ring LAN	57
Figure 29: Hard Wired LAN With Wireless Users	58
Figure 30: Wireless Between User and Multistation Access Unit.....	59
Figure 31: Hard Wired LAN With Wireless Connection Between Server and MAU	60
Figure 32: Wireless Between Server and Multistation Access Units	61
Figure 33: Wireless Between Multistation Access Units	63
Figure 34: Hard Wired LAN With Wireless Connection to Campus Backbone	64
Figure 35: Wireless Between Backbone and Ingersoll LAN	65
Figure 36: By-passing Access Controls; Frequency Hopping algorithm Known	67
Figure 37: Intrusion Inside the Firewall; Frequency Hopping Algorithm Known.....	69
Figure 38: Direct Connection to Wireless Users; Frequency Hopping Algorithm Known	70
Figure 39: IP Spoofing Between MAUs; Frequency Hopping Algorithm Known	72

Figure 40: Denial Of Service; Frequency Hopping Algorithm Not Known	73
---	----

LIST OF TABLES

Table 1: Elements of Secure Public Communications	27
Table 2: Transmission Technology Axis Criteria.....	45
Table 3: Transmission Technology Evaluation	46
Table 4: Axis “d” Criteria For Topology Evaluation.....	48
Table 5: Topology Evaluation	49
Table 6: Vendor Topology Axis Criteria	52
Table 7: Vendor Topology Evaluation	53

I. INTRODUCTION

A. WIRELESS LOCAL AREA NETWORKS

Wireless local area networks (WLANs) are a new alternative to traditional hard wired local area networks (LANs). They use radio frequency (RF) or infrared (IR) transmissions to communicate information from one point to another and do not rely on physical connections. A typical WLAN configuration includes a transceiver (transmitter/receiver) called an access point (AP) connected to the wired network using standard cabling. An access point antenna is mounted anywhere practical to obtain desired coverage. End users access the WLAN through adapters, such as notebook PC cards, that interface between the client network operating system (NOS) and the user.

1. Advantages of wireless over wired

WLAN technologies have been available since 1980, but the increasing number of portable computers has heightened the need for this technology. These systems allow users to access shared information without physically "plugging into" a network, so LAN managers can set up or augment their networks without installing new wires. Advantages offered by WLANs are mobility, low installation costs, installation speed, and scalability.

a. Mobility

WLANs can provide continuous network access to users within their organization thus supporting productivity not possible with wired networks. People can physically move their node (computer) without breaking their virtual network connection. This will be termed "roaming".

b. Low Installation Costs

WLANs offer an advantage over wired LANs where the physical makeup of a building makes it difficult to route wire. Not routing wire yields lower installation costs and quicker setup times. Overall life-cycle costs are also lowered, because there are fewer cables to replace during future upgrades.

*c. **Installation Speed***

Installing a wireless LAN system is faster than installing a hard wired system. The need to pull wire through walls and ceilings is eliminated. Small transceiver type devices are attached to mobile users and the network effectively linking system resources. Wireless technology allows the network to go where wire cannot go.

*d. **Scalability***

Hardware peripherals can be added to the network to serve additional wireless clients. Once the number of clients reach their maximum, extra APs and extension points can be installed to accommodate these users.

2. Department of Defense Applications

Wireless technology can be used in Department of Defense (DoD) applications. Wireless networks can be used in combination with cabled LANs: machines requiring mobility are connected wirelessly, while others remain hard wired. Wireless computing has the potential to reduce costs of routing and maintaining cable and associated hardware peripherals. It can also be configured in a variety of topologies to meet specific application needs. These topologies range from peer-to-peer, suitable for a small number of users, to full infrastructures encompassing thousands of users. WLANs frequently augment, rather than replace, wired LANs, often providing the final few meters of connectivity between a wired network and the mobile user.

B. PROBLEM STATEMENT

Protecting WLANs from attack by malicious hackers and unauthorized users is a problem. Architectural considerations for the inclusion of wireless components into hard wired networks must be addressed. Administrative security and the protection of data should be considered during initial system planning.

C. THESIS OVERVIEW

Flexibility and mobility make wireless LANs both effective extensions to and attractive alternatives for wired networks. WLANs provide all of the connection functionality of wired LANs without the spatial constraints of a physically wired system.

Their configurations range from simple peer-to-peer topologies to complex architectures all offering the benefits of roaming. They offer both end-user mobility and network portability.

Security within information systems is vital to protecting data against exploitation from outside sources. DoD WLAN goals can be addressed by first understanding available technologies and how they may be used securely, and then choosing appropriate vendors to supply the equipment.

Available wireless technologies will be examined to better understand how their use might increase the threat to security. An evaluation of their advantages and disadvantages will show their architectural strengths and weaknesses. These technologies encompass multiple transmission techniques, general security differences, and applicable standards. A final evaluation narrows the field of possible topology and vendor candidates suitable for DoD architectures.

This paper will survey various technologies used to build WLANs in Chapter Two and how WLANs can be protected. Types of attacks and methods to combat them are explored in Chapter Three, culminating in an analytical survey of acceptable WLAN component combinations in Chapter Four. This information provides the basis for a case study, also in Chapter Four, of a typical LAN found at the Naval Postgraduate School. It shows the options available for replacing hard wired segments with wireless. Chapter Five presents final conclusions and discussions.

II. BACKGROUND

Hard wired LANs are used for sharing computer resources and providing connectivity. The WLAN provides an alternative to traditional twisted pair, coaxial cable, and optical fiber based networks. WLANs perform the same function as wired LANs by conveying information among networked devices, but operate without attached physical cabling between nodes. They can be implemented as an extension to, or an alternative for, a wired LAN. WLANs use radio frequency (RF) and Infrared (IR) technology for intercomponent communication. They minimize the need for wired connections and combine data connectivity with user mobility. This chapter will show the transmission, topology, and vendor technologies available to build a WLAN.

A. TECHNOLOGY OVERVIEW: WIRELESS TRANSMISSION TECHNIQUES

Wireless LANs were introduced in 1980.¹ Transmission types include narrowband microwave, infrared, or spread spectrum technologies. Each technology has its advantages and limitations. They are described below.

1. Narrowband Microwave

During radio frequency transmissions, RF data is superimposed (modulated) onto an outgoing radio carrier and then extracted at the receiving end. The radio receiver tunes in one radio frequency while rejecting all others. Multiple radio carriers can coexist without interference if the signals are transmitted at different frequencies. Narrowband radio systems transmit and receive information on specific radio frequencies and are used to interconnect LANs between buildings. They require line-of-sight antenna dishes on both ends of the link. The transmitter encodes an input signal that is mixed with a constant frequency known as the "carrier". The receiver filters out this carrier signal to recover the original data. Narrowband radio keeps the signal frequency within a small specified range. Undesirable crosstalk between communications channels is

¹Sami Uskela, *Security in Wireless Local Area Networks* (http://www.tcm.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html#IntegrityandConfidentiality)

avoided by carefully coordinating different users on different channel frequencies. Communication privacy and noninterference are accomplished by using separate radio frequencies. The radio receiver filters out all radio signals except those on its designated frequency.²

a. *Advantages*

Narrowband microwave radio antennas bypass telephone company lines, so the cost of phone line service is avoided. The antenna itself costs very little, but prices vary depending on size and wattage requirements. Unlike IR, its signal is not easily blocked by physical structures.

b. *Disadvantages*

Narrowband technology is susceptible to interference and is therefore individually licensed by the FCC to prevent other systems from operating at the same frequency in a particular area. Once a site license is granted that frequency band cannot be licensed anywhere else within a 17.5 mile radius. Also, if the frequency is known to a third party, communications can be intercepted.

2. Infrared

Infrared uses the same technology as television remote control units. IR signals transmit data between nodes using either a point-to-point or a sun-and-moon configuration (signals are diffused by reflecting them off of a surface). IR systems use very high frequencies just below those of visible light in the electromagnetic spectrum. Like light, IR cannot penetrate opaque objects. It is either directed (line-of-sight) or reflected.³

² Proxim, *What is a Wireless LAN?* (<http://www.wirelesslan.com/wireless/>).

³ Ibid.

a. *Advantages*

IR is not bandwidth limited and can be used to transmit at speeds greater than 50 Mbps. Range security is inherent due to its inability to penetrate solid objects. IR also does not require an FCC license.

b. *Disadvantages*

Infrared's easy obstruction also acts as a disadvantage when installed in a space with many obstacles. Similarly, its limited range acts as a disadvantage when the WLAN is needed over a large area. Inexpensive systems provide approximately three feet of coverage and are typically used for personal area networks. High performance IR is impractical for mobile users and is therefore used in fixed sub-networks. Diffused (reflected) IR does not require line-of-sight, but cells are limited to individual rooms.

3. *Spread Spectrum*

Most wireless LANs use spread-spectrum technology. It is a wideband RF technique developed by the military for reliable, secure, mission-critical communications systems. It was initially created to avoid jamming and eavesdropping of signals. Spread spectrum exchanges bandwidth efficiency for reliability, integrity, and security. It spreads the signal over a range of frequencies consisting of the industrial, scientific, and medical (ISM) electromagnetic spectrum bands. It avoids concentrating power into a single narrow frequency band. This "spreading" makes the signal appear like noise making the signal bandwidth much larger than that of the original signal. More bandwidth is consumed than in a narrowband transmission, but the tradeoff produces a louder signal that is easier to detect. Spread spectrum frequency bands include frequency ranges at 902 MHz to 928 MHz and 2.4 GHz to 2.484 GHz. The 2.4 GHz range is available worldwide which provides convenient high speed wireless capabilities to users. The FCC regulates the frequency band used by spread spectrum, but does not require individual licensing for local coverage areas. Products developed for unlicensed FCC use must employ one of the two spread spectrum technologies: frequency hopping and direct sequence.⁴

⁴ Ibid.

a. Frequency Hopping Spread Spectrum

Frequency hopping spread spectrum (FHSS) transmits short radio bursts on one frequency then randomly "hops" to another for the next short burst. The carrier signal changes frequency in a pattern known to both transmitter and receiver. The transmission source and destination must also be synchronized, so they are on the same frequency simultaneously. A transmitted message can only be fully received if the series of frequencies is known, because only the intended receiver knows the transmitters hopping sequence. To an unintended receiver, FHSS appears to be short-duration impulse noises. Any radio with a digitally controlled frequency synthesizer can be converted to a frequency hopping radio. This conversion requires the addition of a pseudo noise (PN) code generator to select the frequencies for transmission or reception. Most hopping systems use uniform frequency hopping over a band of frequencies. This is not absolutely necessary if both the transmitter and receiver know in advance what frequencies are to be skipped. A frequency hopped system can use analog or digital carrier modulation. Most vendors develop their own hopping-sequence algorithms which significantly reduces the likelihood that two transmitters will not hop to the same frequency at the same time.⁵

1). Federal Communication Commission Guidelines.

Hopping patterns and dwell times (time at each frequency) are restricted. The Federal Communication Commission (FCC) requires that 75 or more frequencies be used at a maximum dwell time of 400 ms. If interference occurs on one frequency the data are retransmitted on a subsequent hop to another frequency. Each channel consists of a frequency width also determined by the FCC. They require that all transmitters not spend more than 0.4 seconds on any one channel every 20 seconds in the 902 MHz band and every 30 seconds in the 2.4 GHz band. They further require that transmitters hop through at least 50 channels in the 902 MHz band and 75 channels in the 2.4 GHz band.

2). IEEE 802.11. IEEE 802.11 limits frequency hopping spread spectrum transmitters to the 2.4-GHz band.

3). The market for frequency hopping spread spectrum.

All FHSS products allow the use of more than one channel in the same area by

⁵ Ibid.

implementing separate channels on different hopping sequences. This allows for many non-overlapping channels.

b. Direct Sequence Spread Spectrum (pseudonoise)

Direct sequence spread spectrum (DSSS) avoids excessive power concentration by spreading the signal over a wider frequency band. The data signal is modified by a wideband spreading signal that the receiver interprets to obtain the original signal. DSSS transmitters spread their signal by mapping data into a pattern of "chips" called chipping codes and then add these redundant data bits to the transmission. At its destination the chips are mapped back into bits, recreating the original data. The longer the chip, the greater the probability of data recoverability and the more bandwidth required. If one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data. To an unintended receiver, DSSS appears as low-power wideband noise and is ignored. The ratio of chips to bit is called the "spreading ratio". A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the net bandwidth available to a user. Overall these spreading ratios are quite small and most 2.4 GHz product manufacturers offer a spreading ratio of less than 20. Like FHSS, a DSSS receiver must know a transmitters spreading code to decipher data. This spreading code allows multiple direction transmitter operation simultaneously without interference. Once the receiver has the entire signal, it removes the chips with a correlator and collapses the signal to its original length.⁶

1). Federal Communication Commission Guidelines

The FCC requires that each signal have ten or more chips limiting data throughput to 2 Mbps in the 902 MHz band and 8 Mbps in the 2.4 GHz band. The number of chips is directly related to a signal's immunity to interference meaning some throughput is sacrificed to avoid interference.

2). IEEE 802.11

IEEE 802.11 imposes a standard of precisely 11 chips for DSSS as opposed to the FCC's requirement of 10 or greater.

3). The Market for frequency hopping spread spectrum

⁶ Ibid.

DSSS products allow more than one channel in the same area. The 2.4 GHz band is separated into several sub-bands, each containing an independent DSSS network. DSSS truly spreads across the spectrum, so the number of independent (i.e. non-overlapping) channels in the 2.4 GHz band is small. The maximum number of independent channels for any DSSS implementation is three.

B. TECHNOLOGY OVERVIEW: WIRELESS TOPOLOGIES

A "network topology" is a set of workstations that communicate with one another. It is the architectural drawing of the physical configuration that represents the network. At its most basic, two personal computers (PCs) equipped with wireless adapter cards can initiate an independent network when within range of one another. This is called a peer-to-peer network (Figure 1) and requires no administration or pre-configuration. Each PC would only have access to the resources of the other and not to a central server.

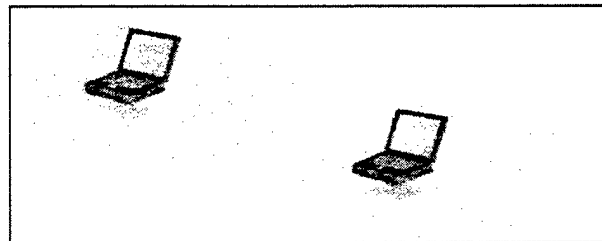


Figure 1: A Wireless Peer-to-Peer Network⁷

Installing a hard wired access point (AP) extends the range of a peer-to-peer network (Figure 2). The AP provides client access to server resources as well as to other clients. Each AP can accommodate many clients dependent upon the amount and nature of the transmissions.

⁷ Ibid.

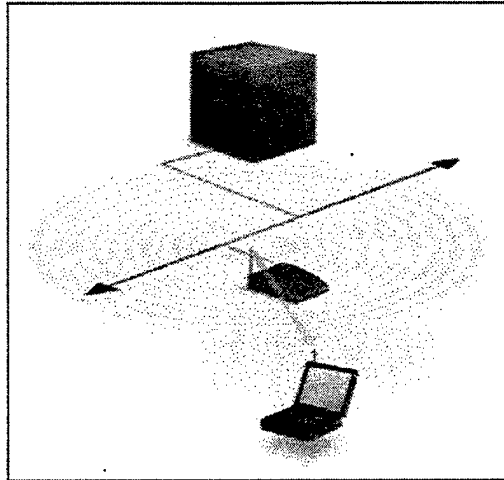


Figure 2: Client and Access Point⁸

Access points have a finite range, so it may be necessary to install multiple APs in large facilities (Figure 3). AP positioning is determined by a site survey. The goal is to blanket the coverage area with overlapping cells, so that users can seamlessly roam throughout the area without losing network contact. APs invisibly hand the user off from one cell to another ensuring unbroken connectivity.

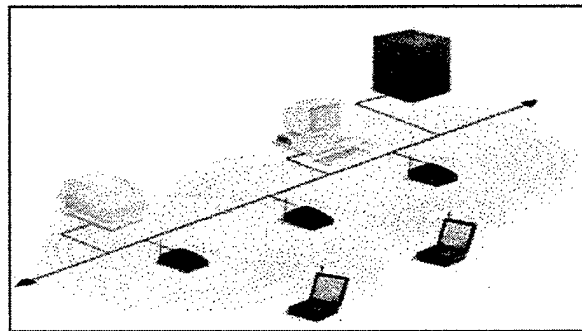


Figure 3: Multiple Access Points and Roaming⁹

To solve extended range problems, Extension Points (EPs) augment the network (Figure 4). EPs function like APs, but are not tethered to the wired network. They

⁸ Ibid.

⁹ Ibid.

extend the range of the network by relaying signals from a client to an AP or another EP. EPs may be strung together to link an AP to far away clients.

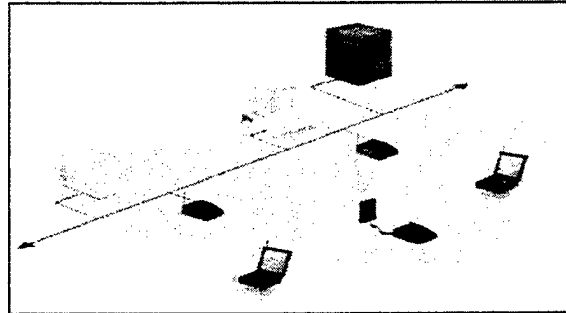


Figure 4: Extension Point Providing Coverage Between APs and Mobile Users¹⁰

A directional antenna extends the WLAN range to other buildings. If a WLAN in building “A” is to be extended to building “B” one mile away, a directional antenna can be installed on each building. Both antennas are connected to WLANs within their buildings enabling wireless LAN connectivity throughout the facility (Figure 5).

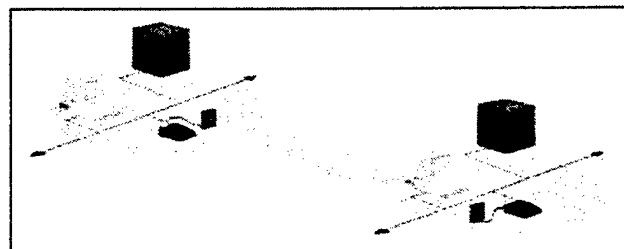


Figure 5: The Use Of Directional Antennas¹¹

Using these examples as building blocks, WLAN topologies can be divided into four distinct categories based on the presence or absence of a network infrastructure.

¹⁰ Ibid.

¹¹ Ibid.

1. Ad Hoc

Ad Hoc networks contain mobile workstations that are wirelessly connected and have no wired infrastructure. They consist of two categories:

a. Ad Hoc without centralized control

Figure (6) is an Ad Hoc network without centralized control where stations send packets directly to each other. Access control is difficult, because unauthorized stations can join the network with no authentication. Additionally, this network is difficult to maintain in large facilities due to range restrictions.

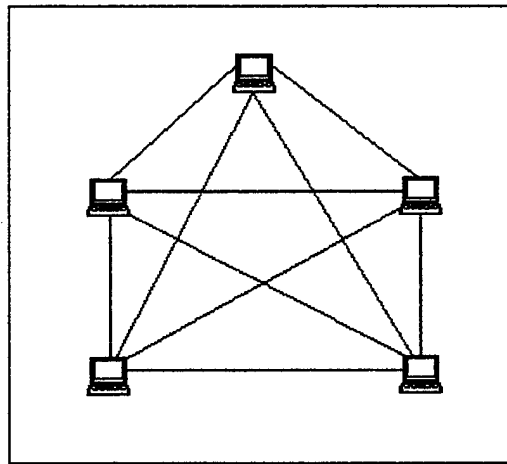


Figure 6: Ad Hoc Without Centralized Control¹²

b. Ad Hoc with centralized control

In Figure (7), the centralized control station is called the Base Station (BS) through which all stations communicate wirelessly. Communication between mobile stations is allowed if restricted access is not imposed by the BS. A problem can arise if

¹² Saraswati Balakrishna, *Network Topologies In Wireless LANs*, (<http://www.cs.umbc.edu/~sbalak1/lan2.html>, December 1995).

one station drifts out of range. The BS is designed to recognize such "drift" and relays a warning message to each mobile unit. Centralized control provides better security, because the BS enforces access control for the mobile units. The level and strength of this control is dependent upon the operating system used in the network.

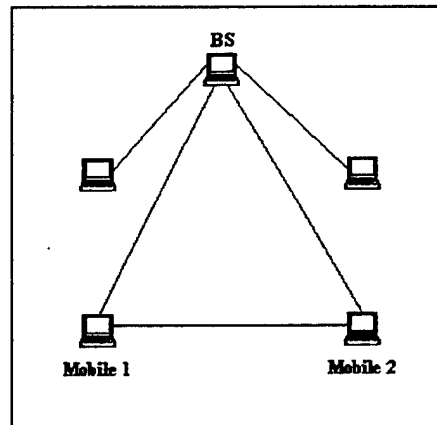


Figure 7: Ad Hoc With Centralized Control¹³

2. Cellular

Cellular networks contain mobile sub-networks that access, either through wired or wireless connections, a base station that is attached to another sub-network (Figure 8). A mobile network can only access one BS at a time and the BS advertises which mobile stations are associated with it. When users roam, a mobile unit may associate itself with another BS creating overlapping BS coverage areas (as in Cell A & Cell B). When this happens the two BSs negotiate between themselves and decide which will assume control of the mobile unit.

¹³ Ibid.

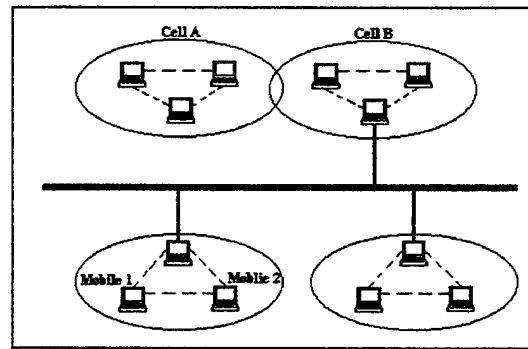


Figure 8: Cellular¹⁴

3. Non-Cellular

Non-cellular networks, shown in Figure (9), are similar to cellular ones, because mobile stations gain access to a wired network through BSs. Unlike the single BS communications in cellular networks, mobile units can simultaneously communicate with multiple BSs increasing communication efficiency. Direct communication between mobile units is not possible, because there is no method for one mobile unit to locate another. There is also no way for the system to know which BS is responsible for which mobile unit. Most WLANs use the Cellular topology for access to wired media.

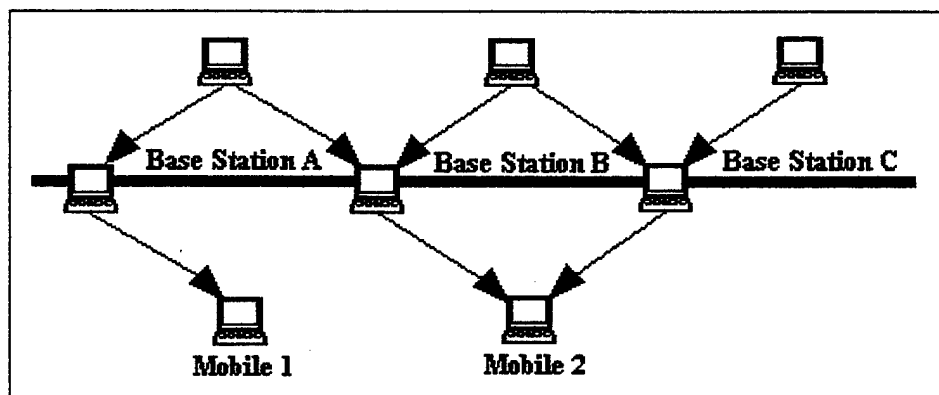


Figure 9: Non-Cellular¹⁵

¹⁴ Ibid.

¹⁵ Ibid.

4. Personal Area Networks

A personal area network (PAN) is used when a small group of computers require access to a set of peripherals (Figure 10). Computers are termed the masters and peripherals the slaves. Slaves respond to commands from the masters. PANs exist in a small geographic area such as an office and are relatively easy to manage.

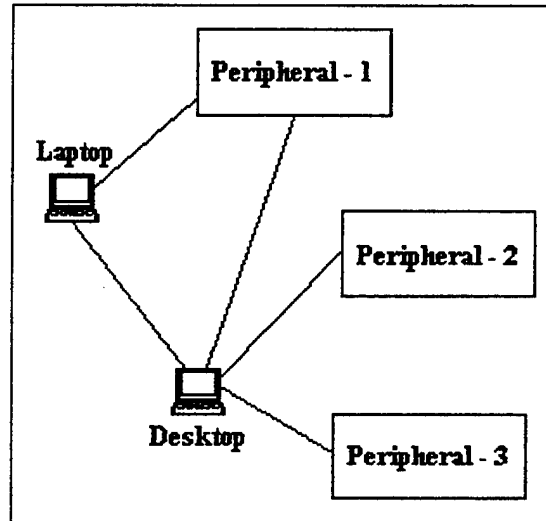


Figure 10: Personal Area Networks¹⁶

C. TECHNOLOGY OVERVIEW: VENDORS

The wireless market is crowded with hardware products that enhance WLAN capabilities. Several vendors provide complete WLAN networking systems with customized services and capabilities.

1. Air-I/O

Telxon Air-I/OTM (Figure 11) spread spectrum WLANs provide office-based communication coverage with data rates up to 2 Mbps. It is 802.11-compliant and is offered in both FHSS and DSSS. Telxon's AirAwareTM Wireless Software provides

¹⁶ Ibid.

connectivity and management tools for the Air-I/O WLAN. AirAware's management tools include AirVision™, AirBeam™, AirGate™ and AirVU™, each of which is described below.¹⁷

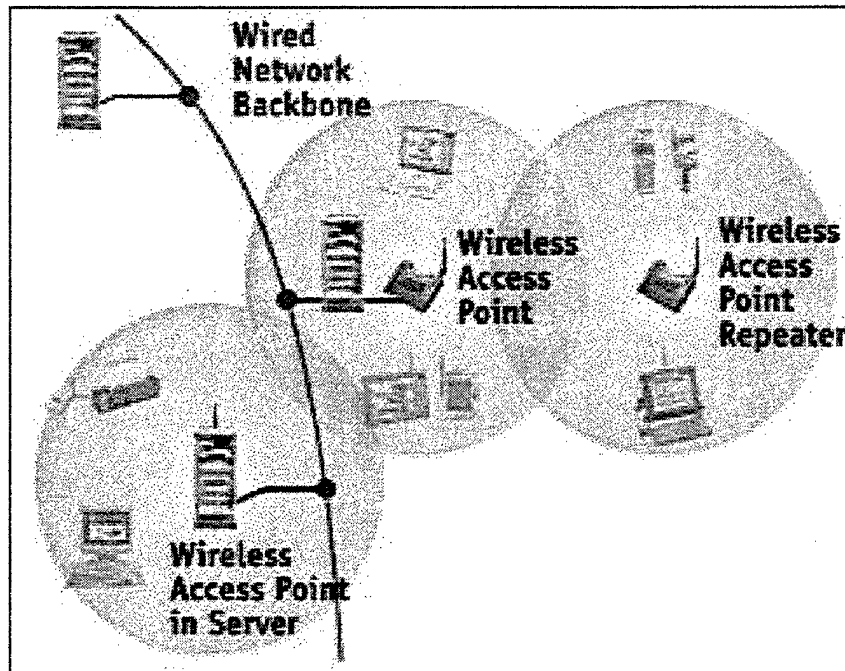


Figure 11: Air-I/O¹⁸

a. AirVision

AirVision helps the user monitor and manage information. Its benefits include remote monitoring, analysis, fault identification, and performance management. AirVision also provides a wired network administrator's management tool that monitors standard terminal connections to wireless devices.¹⁹

¹⁷ Telxon, *Airware Software*, (<http://www.telxon.com/pandtech/wirelessnet/wireless-soft>, 1998).

¹⁸ Ibid.

¹⁹ Telxon, *Airware Software*, (<http://www.telxon.com/pandtech/wirelessnet/wireless-soft/airvision.asp>, 1998).

b. *AirBeam*

AirBeam automates the updating and distribution of mobile client software. It is a set of client-resident executables and API Libraries functioning as a standalone utility on each workstation. AirBeam tracks the application software resident in wireless mobile units and automatically manages software updates as they occur. These updates occur transparently through RF signals.²⁰

c. *AirGate*

AirGate provides wireless gateway application server software. It uses a three-tier client server architecture with a gateway application server placed between the wireless client and connected hosts. Client devices communicate with the server which communicates with data sources and applications on behalf of the client.²¹

d. *AirVU*

AirVU provides standard terminal connection to wireless devices. It uses TCP/IP for direct session communication on host systems thereby not requiring a controller or gateway server. AirVU can also be loaded on handheld devices providing services without restricting the devices other uses.²²

2. Jaguar

Jaguar's 3.2 Mbps WLAN for Ethernet (Figure 12) uses FHSS and offers:

- 3.2 Mbps data rate.
- Equalization that reduces retransmission's and improves throughput.
- Compact designs and miniaturized dual internal antenna systems that are fully embedded into the WLAN PC Card adapter.

²⁰ Telxon, *Airware Software*, (<http://www.telxon.com/pandtech/wirelessnet/wireless-soft/airbeam.asp>, 1998).

²¹ Telxon, *Airware Software*, (<http://www.telxon.com/pandtech/wirelessnet/wireless-soft/airgate.asp>, 1998).

²² Telxon, *Airware Software*, (<http://www.telxon.com/pandtech/wirelessnet/wireless-soft/airvu.asp>, 1998).

- PC Card Link Status Indicator that tells the user when the mobile unit is within range of an AP and the received data rate performance.
- Wireless LAN cell hand-offs .

Jaguar products are “plug and play” operating in the unlicensed 2.4 GHz frequency band. It dynamically selects between two digital modulation techniques, QPSK and 16QAM, to deliver the maximum data rate possible. In QPSK mode, Jaguar delivers a raw data rate of 1.6 Mbps and user data throughput of 1.1 Mbps. In 16QAM mode, it delivers a raw data rate of 3.2 Mbps and a maximum user data throughput of 2.2 Mbps.²³

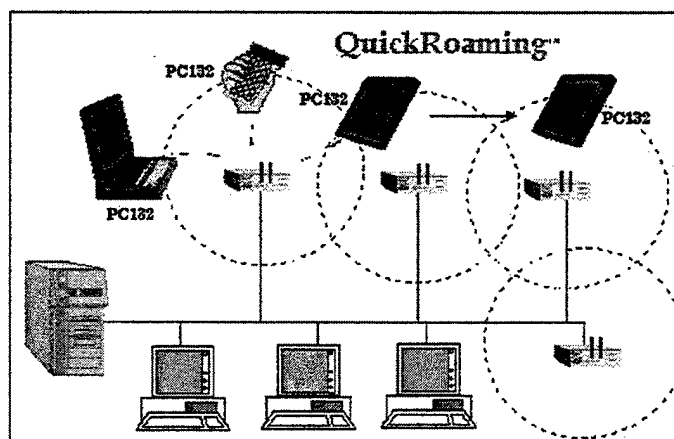


Figure 12: Jaguar's 3.2 Mbps Wireless LAN²⁴

Jaguar is hub-based using a WLAN AP that provides the interface to a wired Ethernet. This AP can also serve as a field BS allowing virtual "networking" without a hard wired connection to the Ethernet. It provides a maximum open air coverage area of 1,500 meters. The maximum coverage area for a cell is determined by the type of obstructions the radio signals pass through, the noise environment, and height above ground. These APs can also use one of 78 different hopping patterns providing

²³ Jaguar, *Echipamente Wireless LAN, JAGUAR: 3.2 Mbps Wireless LAN for Ethernet*, (http://www.agerd.ro/produse/wireless/jaguar_topo.html, September 1998).

²⁴ Ibid.

maximum flexibility for network expansion. Each WLAN cell supports up to 62 users with load-balancing capabilities that automatically distribute these users among various overlapping cells. Jaguar can support up to 15 overlapping cells before data rate performance degrades. If cells do not overlap, network extension is indefinite (Figure 13).

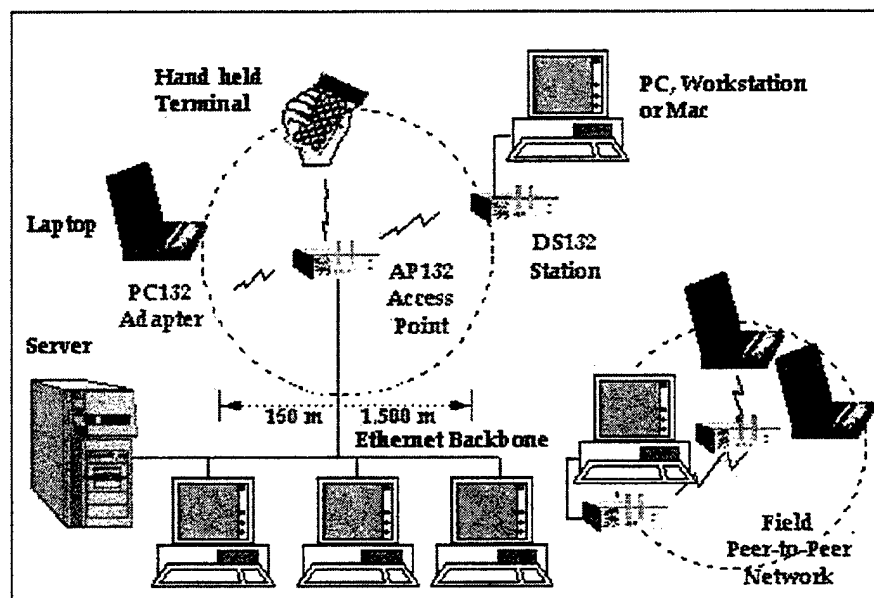


Figure 13: Jaguar Access Point Configuration²⁵

3. WaveLyNX BR132™

WaveLyNX BR 132 is an Ethernet WLAN bridge system that supports a point-to-point topology. It establishes dedicated connections between two LANs. BR 132 supports 3.2 Mbps up to six miles and a 2.4 Mbps user throughput to a maximum single-hop range of 20 miles. In noisy environments, it automatically falls back to 1.6 Mbps and links over 20 miles are supportable using a repeater. BR 132 uses WaveAccess' Adaptive Equalization (ADEQ)[™] technology as well as Quadrature Phase Shift Keying (QPSK) and 16 quadrature amplitude modulation (QAM) modulation, rather than simple frequency shift keying (FSK). ADEQ allows more effective operation in noisy multipath environments. BR 132s are deployed in pairs and are pre-configured as master and slave with factory default hopping pattern settings for "out-of-the-box" operation. Each

²⁵ Ibid.

BR 132 also comes with a pair of standard 2 dBi gain antennas which are used for simple communication links between LANs. Actual link speeds are determined by the distance covered, antenna type, cable type, and cable length (Figure 14).²⁶

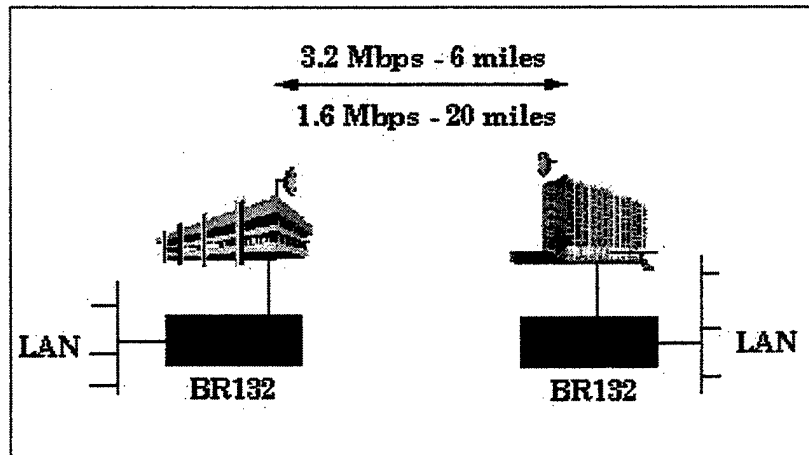


Figure 14: WaveLyNX BR 132²⁷

4. NetWeaver

NetWeaver is a high-performance, digital, point-to-multipoint data communication system that provides high-speed wireless networking. It operates at 2.4 GHz FHSS offering full-duplex operation within each channel scaleable to 3.2 Mbps. It has a variable range to a maximum of 10 miles (Figure 15).²⁸

²⁶ WaveLyNX, *Echipamente Wireless LAN: WaveLyNX BR132 Network Topology*, (http://www.agerd.ro/produse/wireless/lynx_topo.html, September 1998).

²⁷ Ibid.

²⁸ WaveLyNX, *NetWeaver: Metropolitan Multipoint Internetworking Systems*, (http://www.agerd.ro/produse/wireless/netweaver_spec.html, September 1998).

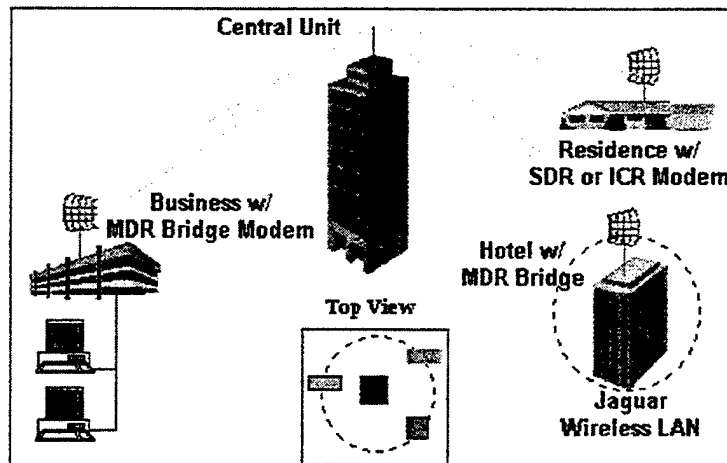


Figure 15: NetWeaver²⁹

NetWeaver is based on a hub and spoke topology. It uses Central Unit (CU) modems that each support a single 3.2 Mbps or 1.6 Mbps channel with links supporting up to 62 wireless remote site radio modems. CUs access the Internet via a wired or wireless backbone and offer two digital wireless modem models:

- SDR 132 Single Drop Remote that supports a single desktop computer via a 10Base-T port through the computer's Ethernet card, or a LAN connection via a router.
- MDR 132 Multi Drop Remote that supports full 802.3 bridging.

NetWeaver remote wireless modems use full-duplex outdoor directional antennas. As network bandwidth requirements increase, additional CU channels can be added: up to 10 channels per base station. CU modules also support both omnidirectional and directional antenna arrays, ensuring that multiple BSs can be arranged for nearly unlimited scalability (Figure 16).

²⁹ Ibid.

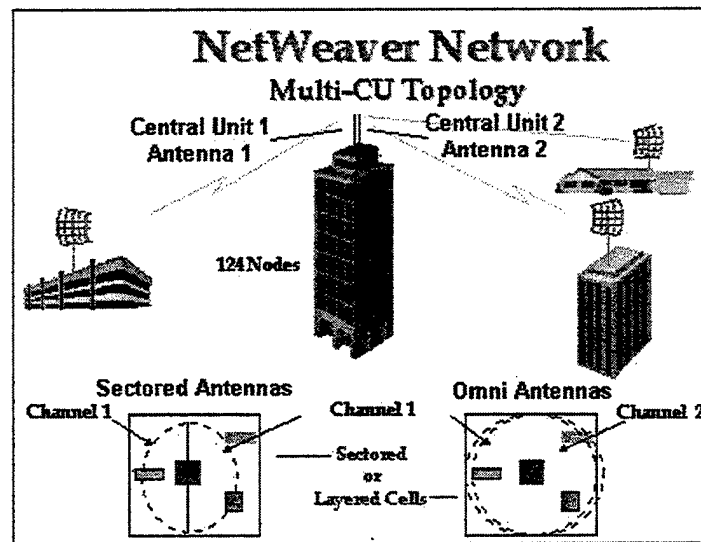


Figure 16: NetWeaver CU Topology³⁰

NetWeaver cells can be augmented or interconnected by WaveLyNX and NetWeavers MDR 132 digital modems can interface with the 3.2 Mbps WaveAccess Jaguar WLAN. This allows for reliable indoor roaming.

³⁰ Ibid.

III. SECURITY CONCERNS FOR WIRELESS

Security for all network types is important. Disgruntled former employees, Internet hackers, and industrial spies are all possible network attackers. How they might use WLANs is discussed in this chapter.

A. GENERAL SECURITY LEVELS

Security levels in wireless communication channels, grouped from most secure to least secure, are defined as:

- Secure Military Systems (JTIDS, MILSTAR, GPS): Wireless military communication systems are used for electronic warfare (EW), electronic countermeasures (ECM), and electronic counter-counter measures (ECCM). Some military systems can counteract jamming (denial of access), spoofing, and detection using anti-jam, anti-spoofing, and low-probability-of-intercept methods.
- Secure Public Systems: Secure public systems provide authentication and data encryption, but other general security issues are not addressed.
- Unsecured Public Systems (POTS, AMPS, Two-Way FM, Broadcast): Plain old telephone service (POTS), broadcast, and cellular phones are unsecured. Advanced mobile phone service (AMPS-Cellular) is protected by regulations against eavesdropping, but this is unenforceable.³¹

1. Secure Military Systems

Modern military forces depend on sophisticated radio communication and navigation systems. An enemy can employ ECM to detect these radio signals and either disrupt or exploit them. Disruption is accomplished by jamming and exploitation by using transmissions for their intelligence value. Prior to development of transmission security, it was possible to gather intelligence from signals by demodulating and decoding them. For some systems it is also possible to "spoof" or provide false

³¹ Steve F. Russell, *Wireless Channel Security Tutorial* (http://www.ee.iastate.edu/~wireless/security/w_tut_1.html, Iowa State University, February 1997).

information (counter-intelligence). A diagram of these ECM techniques is shown in Figure (17).

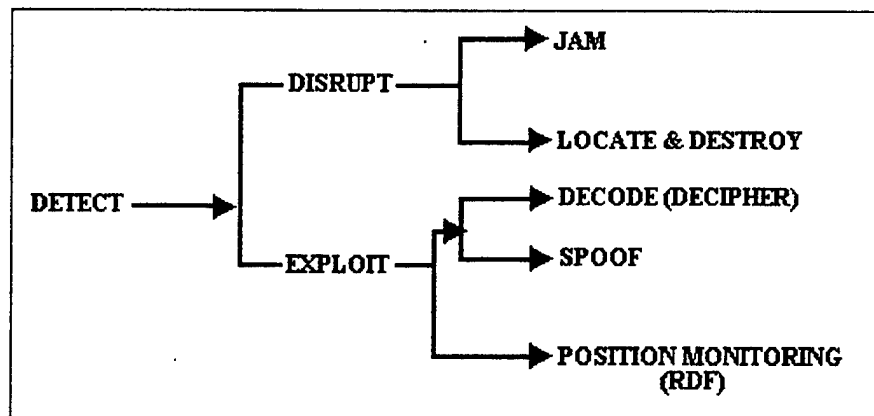


Figure 17: Electronic Warfare Overview for Military Systems³²

Alternate terminologies that describe ECCM concepts include Low Probability of Detection (LPD), Low Probability of Exploitation (LPE), and Low Probability of Intercept (LPI). LPD prevents the enemy from detecting a radio transmission and minimizes power spectral density and detectability. LPE prevents the exploitation of signals by decoding, spoofing, or position monitoring. It denies the enemy knowledge of the system, its modulation characteristics, its use, and its users. LPI encompasses both LPD and LPE and is a generic term from which the term “anti-intercept” is derived.

2. Secure Public Systems

The typical public WLAN system is shown in Figure (18). The public network (Internet) and the private network (university) are usually not secure. The private network (industry), the wireless service provider, and a private LAN are usually secure. Figure (18) also illustrates security firewalls for secure private networks.

³² Ibid.

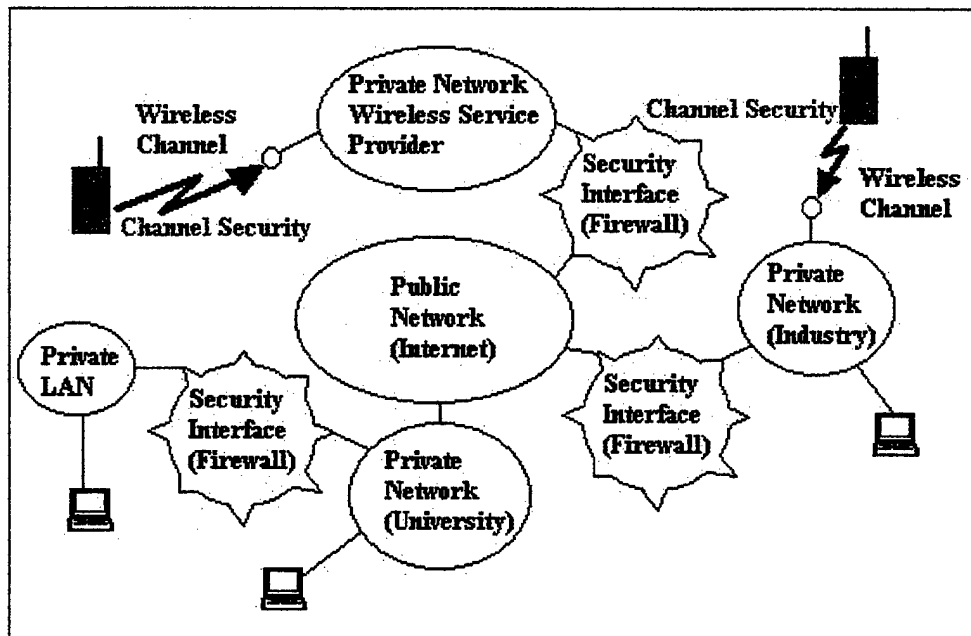


Figure 18: Wireless Public Information Network³³

Wireless channels are protected only by data encryption, authentication, and limited protection to elementary attempts at jamming, spoofing, and interception. Channel security characteristics for secure public communication systems are grouped into categories shown in Table (1). It shows the ECM and ECCM techniques used to combat malicious attacks:

Elements of Secure Public Communications		
ECM	UTILIZATION	ECCM
Detection	Determine Presence and Activity of RF Signal	Anti-Intercept
Location	Monitor and Track Position of RF Signal	Anti-Intercept
Denial of Service	Disrupt or Deny Use to Unauthorized Users	Anti-Jam
Counterfeiting	Theft of Services by Unauthorized Users	Encrypted Authentication
Decoding	Obtain Information from Attacker	Data Encryption
Spoofing	Supply Deceptive Information to Attacker	Spoofing Security

Table 1: Elements of Secure Public Communications³⁴

³³ Ibid.

³⁴ Ibid.

Detection determines activity and patterns of use and is the first step in employing additional ECM techniques. Location locates and tracks wireless transmitters within the network. Some programs locate a cell phone user down to the cell site and antenna sector level. Denial of Service is used in the public system to disrupt or deny use to unauthorized users. Counterfeiting results in illegal or unauthorized access to services. Decoding digital voice and data is the least important, because data encryption methods are well advanced and can mitigate this threat. Spoofing security is a developing area of ECCM research and supplies deceptive information to an attacker. One example utility is the Deception Toolkit from Fred Cohen and Associates.³⁵

B. LOGICAL ACCESS

Anyone gaining access to a typical commercial-off-the-shelf (COTS) wired LAN can potentially damage the network or compromise the integrity of its information. Without proper security measures, even authorized users might gain unauthorized access restricted information. In WLANs, wireless channels are shared by multiple users creating the need for a media access control (MAC) protocol to coordinate access. In the open system interconnection (OSI) model of communications (Appendix A) the MAC function is a sublayer of the Data Link Layer. Each transmitted packet contains a source and destination address. Packets with recognized destination addresses stay on the LAN while unrecognized packets are presumed destined for another network and are forwarded. LAN/WLAN MAC protocols include random access protocols (ALOHA or Carrier Sense Multiple Detect [CSMA]), reservation techniques (a protocol similar to RTS/CTS [Request-To-Send/Clear-To-Send]), or a combination of the two (Time Division Multiple Access [TDMA]).

C. ATTACKS: LAN VERSUS WLAN

WLANs possess the same security problems as wired LANs, but new security concerns emerge when using radio communications. Data transfers can be compromised by sniffers, radio frequency “grabbers”, and stray emissions. Intentional or unintentional jamming, spoofing, and eavesdropping can degrade WLAN security. New questions emerge: can WLANs exist side-by-side without interference? Do they interfere with

³⁵ Fred Cohen and Associates, *The Deception Toolkit* (<http://www.all.net>).

other nearby radio frequencies? How are nearby cell phone communications affected? How do cell phones affect WLAN communications? Many of these threats to communications security can be mitigated by cryptographic systems that encode data, thus providing secrecy and sender authentication, and by firewalls that stop electronic intrusion.

Common LAN attacks can be grouped into four categories:

- 1) Interruption: This attack makes LAN resources unavailable by interrupting service. It can be employed by excessively pinging the network from an outside Internet address or by physically cutting system cables.
- 2) Interception: This attack captures data about sender and receiver identities. An example is data that can be used to exploit personal information about the user or to use their address for gaining access to the network.
- 3) Modification: This attack modifies captured data and sends it to unsuspecting users to trick them into performing actions that are beneficial to the attacker.
- 4) Fabrication: This attack falsifies an attackers identity to lure authorized users into providing information useful to the attacker.

Of greater concern to the wireless system are RF attacks between APs rather than data manipulation of the actual packet. These attacks are derived from traditional categories listed above and are broken down into more detailed wireless classifications:

- Eavesdropping
- Transitive Trust
- Infrastructure
- Denial of Service

1. Eavesdropping

Eavesdropping occurs when an attacker unjustly receives transmissions intended for someone else. Any receiver within range, outside or inside of the building, can eavesdrop on a message. The equipment required to eavesdrop is reasonably priced and authorized users cannot detect that the transmission has been compromised. Transceiver power and frequency band affect the range where the transmission can be heard. When a transceiver operating at greater than or equal to 2 MHz powers up, traffic can be

eavesdropped from outside of the building unless special electromagnetic shielding is used.³⁶

2. Transitive Trust

Paths of communication that require trust between nodes within the same network can be the target of a transitive trust attack. Specifically, if node "A" trusts "B" and B trusts "C", then A trusts C. Often, A does not know that it trusts C. These relationships can be bi-directional, so the security of a path is equal to the security of the weakest node.³⁷ A WLAN AP is the gateway for a transitive trust attack. Once the WLAN is fooled into trusting an attacker's computer, the attacker gains access to all systems behind the network firewalls. Wired networks physically constrain signals between nodes, but there is no way to physically track wireless signal identity during transmission. The only current protection is standard IP addressing or a trusted authentication mechanism between mobile assets.³⁸

3. Infrastructure

Infrastructure attacks are launched against internal system weaknesses including software bugs, configuration mistakes, and hardware failures. These occur in WLANs, but attack protection is almost impossible. A bug is not discovered until something bad happens, so the only recourse is to minimize damage.

4. Physical Denial of Service

WLANs are vulnerable to physical denial of service attacks. A powerful attacking transmitter can generate interference from outside of the site rendering the WLAN useless. The only complete protection is to use the WLAN within a Faraday cage

³⁶ Sami Uskela, *Security in Wireless Local Area Networks* (http://www.tcm.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html#IntegrityandConfidentiality, Department of Electrical and Communications Engineering, Helsinki University of Technology, December 1997).

³⁷ *Standard Department of Defense Trusted Computer System Evaluation Criteria*, (<http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html#HDR6.3>, DOD 5200.28-STD, December 1985).

³⁸ *Ibid.*, p. 6.

(a conducting cage that shields electronic equipment). Authorities can locate the offending transmitter for as long as the attack continues.

D. ANALYSIS OF TOOLS WITHIN THE WIRELESS CONTEXT

The above active attacks show possible weaknesses of wireless networks. There are many tools that exploit these vulnerabilities and most are free on the Internet. Intrusion detection tools are also available, but require diligence in their implementation. Hacker and intrusion detection tools are discussed here. It is important to understand how they work, so that less vulnerable wireless networks can be designed. This overview of tools will further help the reader understand the security analysis described in the case study.

1. Hacker Tools in WLANs

Malicious hacker tools evolve as network loopholes are discovered. Their proliferation within the wired LAN environment is testimony to their impending use within WLANs. They may all be used to attack WLANs and the attacker can easily hide by logging on remotely. Some of the better known and therefore more frequently used tools of the network hacker are described below.

a. *Satan*

The "Satan" (Security Administrator Tool for Analyzing Networks) LAN administrative tool is powerful and easy to use, but can also intrude on and degrade network security. It reports security weaknesses in networks by intruding the same way an attacker would: from a host that is not part of the LAN. An administrator can discover many security holes and repair them. Satan can make systems more secure, but a site's administrators must use and act on its results before an attacker does. A skilled programmer can modify it making it intrusive, as the product is distributed with complete source code. It is also user friendly. Its graphical user interface (GUI) is so easy to use that less experienced hackers can operate it.³⁹

³⁹ Clinton Wilder and Jason Levitt, *Cure Or Curse?*, (<http://www.iweek.com/521/21m/sat.htm>, April 1995).

b. Back Orifice

Back Orifice (BO) is a Windows 95 administration system that allows users to control network machines remotely. From a remote LAN or the Internet, BO users have more control of a network machine than the person at the keyboard of that machine. After self installation is complete the executables are placed into the system where it avoids interference with other applications. After system power up, BO does not display on the task or close-program list and reruns every time the computer is started.

Back Orifice's capabilities are numerous. Network resources and lists of incoming and outgoing connections can be viewed. Network connections can be created and deleted. Exported resources and their passwords can be listed, created, and deleted. TCP ports can be redirected and files uploaded and downloaded on any port using a web browser. Files and directories can be copied, renamed, deleted, viewed, and searched. It also lists, creates, deletes, and sets keys and values in the registry.⁴⁰

c. Internet Protocol Spoofing

Internet Protocol (IP) spoofing hides a true IP address on Ethernet networks while making it appear to have an entirely different address. Blind spoofing is available on all other networks meaning an attacker cannot see which remote host is responding. During blind spoofing the remote host responds to the fake address. The attacker, therefore, never sees this response.⁴¹

d. L0pht Crack

L0pht Crack is a Windows 95/NT password cracker and auditing tool created by L0pht Heavy Industries. Maj. V. Glenn Schoonover, Chief, Network Security, Single Agency, Manager for Pentagon IT Services stated, "No kidding, this is one bad tool. We ran this against a base of 5,000 users and it cracked passwords that had previously been uncrackable."⁴²

⁴⁰ Jim Williams, Hacker Tools, (<http://netsecurity.miningco.com/msub19.htm>, December 1998).

⁴¹ Ibid.

⁴² Ibid.

L0phtCrack 2.0 is shareware and was originally envisioned as an experimental research tool. The trial period is 15 days after which the product must be registered for \$50. A stripped down version with source code is available for free.

e. NT Recover/Locksmith

NT Recover/Locksmith accesses WinNT computers through a serial connection. It can change the administrators password when the original password has been lost. NT Recover/Locksmith has a 100% success rate and gains entry within minutes.⁴³

f. Snadboy's Revelation

Snadboy's Revelation uncovers passwords that Windows 95/98 have hidden behind asterisks. Users can also reclaim previously deleted passwords. Snadboy's Revelation is freeware, but the source code is available for \$150.00.⁴⁴

g. Password Hacker

Password Hacker is similar to Snadboy's Revelation by revealing passwords normally hidden behind asterisks.⁴⁵

h. Portscan

Portscan allows scanning for open ports on a host in a specified port range. For example, if the host "microsoft.com" and then the port range from 50 to 150 are entered, the user may get port 80 in an output text box. This shows that a Web server is running on that host.⁴⁶

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ Ibid.

⁴⁶ Ibid.

i. Sniff it

Sniffet is a packet sniffer used on UNIX, Linux, FreeBSD, and Irix systems. It listens to all TCP/IP traffic on a subnet, intercepts outgoing and incoming requests for Web documents, and decodes authentication passwords. Its scripts wrap around the UNIX tcpdump network debugging utility which comes pre-installed in UNIX. These scripts will not work on Windows or Macintosh systems, because tcpdump is not available on these platforms.⁴⁷

2. Intrusion detection tools

Intrusion detection is currently being used as a panacea - a poor substitute for well engineered solutions. Previously described attacks cannot be countered without knowledge that the attack is occurring. Below the most common intrusion detection tools and their capabilities are described.

a. Intruder Alert Version 3.0

Intruder Alert Version 3.0 "...monitors and responds to information system threats in real-time across distributed computing platforms."⁴⁸ It automatically detects attacks, unauthorized activity, and network abuse from both internal and external sources. Intruder Alert uses a centralized audit information collection and audit reduction capabilities. Intruder Alert runs in the Windows NT background and detects real-time system events by monitoring audit logs. It then sends a warning email to the administrator and establishes secure communications with the Manager component using a 400 bit Diffie-Helman key. Once authenticated, an algorithm encrypts the Agent's communications.

⁴⁷ Ibid.

⁴⁸ Steven R. Balmer and Rett Shirley, *Intrusion Detection Technology Experiences with Axent Intruder Alert*, (Naval Postgraduate School, August 1998).

b. *ISS REALSECURE Version 2.5*

ISS REALSECURE is a host based network traffic analyzer with a unique attack recognition engine. It's components include a console and multiple engines. The console gathers information from engines that are running throughout the network. These engines leave no evidence that they are active.⁴⁹

c. *Kane Security Monitor 3.13*

Kane Security Monitor watches the network and provides an alarm for intended intrusion, obvious violations, and irregularities in user behavior. It also analyzes security event logs on servers and workstations. Kane's agent service collects data based on matched security patterns from event logs and passes it to an auditor service. From his console, an administrator can easily install an agent on any NT server or workstation.⁵⁰

d. *Session Wall-3*

Session Wall is a sniffer that detects network abuses. It can generate a complete picture that sees the network one packet at a time. It only monitors the segment to which it is attached and monitoring of multiple segments requires installation of multiple network cards. It is best placed on either side of the firewall or network point of entry to the Internet.⁵¹

⁴⁹ Larry Brachfeld, Jimmy Francis, Dan Morris, and Scott Robin, *Evaluation of RealSecure*, (Naval Postgraduate School, CS3670, November 1998).

⁵⁰ Enno Busch, Murat Akbay, and George Floros, *Intrusion Detection System (IDS) Project 1 Report*, (Naval Postgraduate School, CS3670).

⁵¹ Dave Hensley, Katrina Hensley, and Les Prior, *Intrusion Detection System Evaluation, Session Wall-3 by AbirNet Inc.* (Naval Postgraduate School, CS3670, November 1998).

E. SECURITY STANDARDS

HIPERLAN and IEEE 802.11 are two WLAN standards that present features to address security vulnerabilities. Many wireless products have no security functions and even IEEE 802.11 labels such functions as optional.⁵²

1. HIPERLAN

The High Performance European Radio Local Area Network (HIPERLAN) standard is the wireless broadband access standard created by the European Telecommunications Standards Institute (ETSI). This standard defines part of the OSI models physical and data link layer (DLL). The HIPERLAN physical layer operates in two frequency bands; 5.15 to 5.25 GHz and 17.1 to 17.3 GHz. Equipment transmitting in the first band may operate a 1W transmitter and the second band with a 100 mW transmitter. A 25 Mbps bit rate at the 5 GHz physical layer can operate on five different channels and can grant users equal access to the spectrum. This supports a wide range of applications. HIPERLAN equipment cannot legally use the two upper channels of the 5 GHz band in some countries.

The MAC HIPERLAN sub-layer is a decentralized sub-system allowing ad-hoc applications. This sub-layer provides equipment interoperability and ensures a level of security against casual eavesdropping. Connectivity within a single HIPERLAN is accomplished at the MAC level by special nodes called "forwarders". When a signal's intended receiver is out of range, forwarders act as extensions that relay packets on to their final destinations.

HIPERLAN's specifications European Telecommunications Standard (ETS) draft was approved by ETSI in February 1995 with the following properties:

- 1) It may be used in pre-arranged or ad-hoc fashion.
- 2) It supports node mobility.
- 3) It may have a coverage beyond the radio range limitation of a single node.
- 4) It supports both asynchronous (no timing requirement for transmission and the start of each character is individually signaled by the transmitting device) and time-bounded communication using a Channel Access Mechanism.

⁵² Ibid.

- 5) Its nodes may conserve communication power by arranging active reception times.⁵³

a. Encryption-Decryption

HIPERLAN defines an optional encryption-decryption scheme. It uses a set of shared keys, referred as the HIPERLAN key-set. Each key has a unique identifier and plain text is ciphered by an XOR operation with a confidential algorithmic pseudo-random sequence. (Figure (19)).

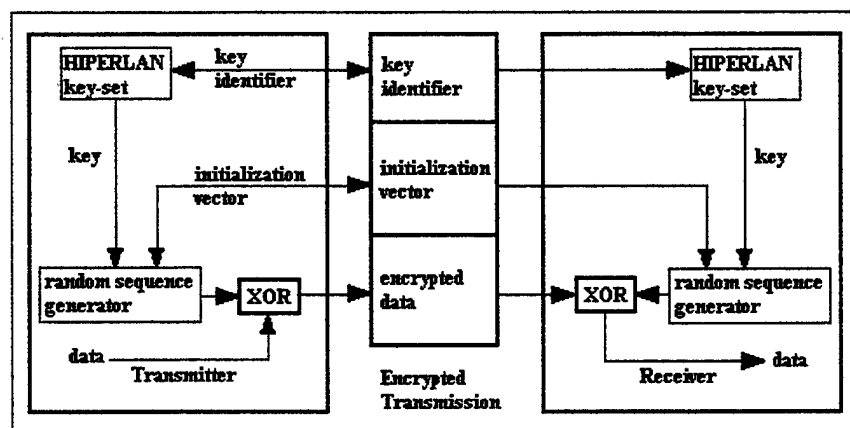


Figure 19: HIPERLAN Encryption-Decryption Scheme⁵⁴

b. Protection

Wired Equivalent Privacy (WEP) protection levels cannot be evaluated here, because they are proprietary. The HIPERLAN standard does not define any authentication, so WEP security should not be trusted in sensitive applications.

2. IEEE 802.11

IEEE 802.11 is the WLAN standard developed by the Institute of Electrical and Electronics Engineers (IEEE). It resolves compatibility issues between manufacturers of

⁵³ Ibid.

⁵⁴ Opinnot, *HIPERLAN encryption-decryption scheme*, <http://www.tcm.hut.fi/Opinnot/Tik-110.50/1997/images/hiperlan.gif>, 1997.

WLAN equipment and products supporting it are already on the market. IEEE 802.11 defines the physical layers and the MAC sublayers for wireless. All physical layers offer a 2 Mbps data rate at the 2.4-2.4835 GHz band. The MAC layer has the following features:

- 1) Supports Isochronous (uniform in time; having equal duration) as well as Asynchronous data.
- 2) Supports priority.
- 3) Association/disassociation to an AP in a Basic Service Set (BSS) (a set of stations communicating wirelessly on the same channel in the same area) or Extended Service Set (ESS) (a set of BSSs and wired LANs with AP's that appear as a single logical BSS).
- 4) Re-association with or Mobility Management to transfer association between APs.
- 5) Power Management to save battery time.
- 6) Authentication to establish terminal identity.
- 7) Acknowledgment to ensure reliable transmission.
- 8) Timing synchronization to coordinate terminals.
- 9) Sequencing with duplication detection and recovery.
- 10) Fragmentation re-assembly.

a. Authentication

IEEE 802.11 defines two authentication schemes: Open System and Shared Key Authentication. The former is a null authentication, because all mobile units are accepted to the network. For the latter, a mobile unit requests authentication and the base sends an encrypted 128 octet (1024 bits) random number to it using a shared key. The unit decrypts the number using the same key and responds. If the base receives the correct number, the mobile is accepted into the network. All accepted mobiles use the same shared key. Mobiles cannot be distinguished between each other and there is no way to authenticate the network by the mobile.

b. Wired Equivalent Privacy

IEEE 802.11 defines an optional Wired Equivalent Privacy (WEP) mechanism to ensure confidentiality and integrity of network traffic. WEP is used at the

station-to-station level and uses the RC4 PRNG (parallel random number generator) algorithm. It uses a 40 bit secret key and a 24 bit initialization vector (IV) send with the data. WEP also includes an integrity check vector (ICV), so the receiver is always able to decrypt the cipher text block. This is illustrated in Figure (20).

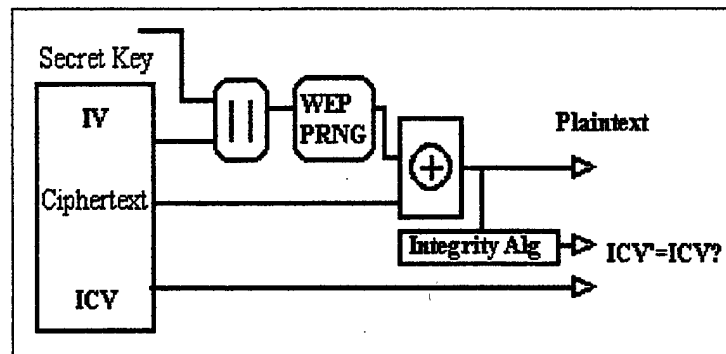


Figure 20: WEP Mechanism⁵⁵

c. *Parallel Random Number Generator Algorithm*

The PRNG algorithm is proprietary, but has been studied in independent research laboratories under nondisclosure agreements. No weaknesses have been reported. However, the secret key can be revealed by using brute-force attack in two seconds with tested \$100,000 hardware and 0.2 seconds with tested \$1,000,000 hardware according to 1995 Figures.⁵⁶

F. CONCLUSION

Diligent security management is important to both wired and wireless LANs. WLANs can take advantage of available wired LAN security measures and add additional features not available in the wired world. Authentication mechanisms may be used over IP to perform end-to-end authentication, but this presents a potential launch pad for an

⁵⁵ Opinnot, *WEP mechanism*, (<http://www.tcm.hut.fi/Opinnot/Tik-110.501/1997/images/ieee2.gif>, 1997).

⁵⁶ Ibid., p. 6.

attacker. The hardware or software based mechanism becomes the only security layer between the network and the attacker. The nature of radio communication makes it practically impossible to prevent some attacks, such as physical denial of service and eavesdropping, but if security is considered while they are being designed, then WLANs can be more secure.

IV. ANALYSIS AND EVALUATION

Network designers and administrators face many technology and hardware options. Available technologies, topologies, and vendors are analyzed using Kiviat diagrams.⁵⁷ These diagrams graphically display analyzed attributes by giving a logical “picture” of the final evaluation. A Kiviat diagram consists of axes originating from a central point in a circular diagram. Each axis represents criteria pertinent to the analyzed category with measured gradients from one to five. Each axis and its measurement are defined prior to the subject category, summarized in a table, and then shown on the Kiviat graph. A perfect evaluation yields a drawing similar to Figure (21). Each subject area may differ in its number of axes, but the number of axes and evaluation criteria are the same within each category. As will be explained in subsequent sections, these categories are considered to be of equal importance. Therefore, they are also equally weighted on the Kiviat scales to provide a balanced analysis. The evaluation scope begins with available transmission technologies, narrows to popular topologies, and then to vendor products.

⁵⁷ Shawn D. James, *Thinking Strategically about information-Based Conflict: Developing an Analytical Approach to Operational Measures of Effectiveness*, (Naval Postgraduate School, Thesis, September 1996), P. 141.

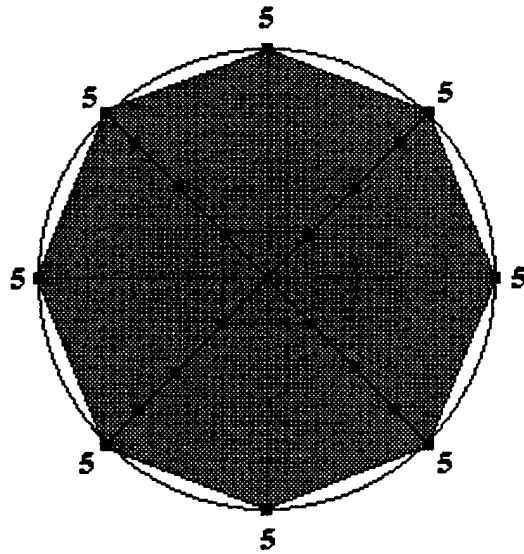


Figure 2 1: Shaded Kiviat Diagram⁵⁸

A. TRANSMISSION TECHNOLOGIES

Narrowband Microwave, Infrared, and Spread Spectrum were explained earlier, but further analysis of spread spectrum capabilities is provided here. Spread spectrum signals are hard to exploit or spoof, making them attractive for military use. Signal exploitation occurs when a non-network member listens to the network and uses acquired information for their own advantage. Spoofing is maliciously introducing unauthorized traffic into a network under a false address. Advantages of FHSS over DSSS are discussed below.⁵⁹

- Throughput: Point-to-point throughput is variable between both DSSS and FHSS products. Protocols for DSSS throughput sacrifice mobility and roaming performance, but FHSS provides greater power, signal efficiency, mobility, and immunity from multipath interference.

⁵⁸ Ibid.

⁵⁹ Proxim White Paper, *Selecting a Wireless LAN Technology*, <http://www.proxim.com/learn/whiteppr/select.shtml>.

•Interception: DSSS data is easier to intercept than FHSS data. Constant hopping of FHSS signals make it less susceptible to interference and interception. DSSS, on the other hand, uses simple spreading codes that allow mapping of transmissions back into original data. Once an attacker is on the DSSS frequency, he need only transform the signal back to its original form by using an appropriate algorithm. Both DSSS and FHSS can be supplemented with specialized encryption devices, but this increases cost, weight and power consumption of the mobile unit.

•Power: FHSS radios use less power than DSSS and have a practical limit of 2 Mbps. Direct Sequences radios rate of 8 Mbps is only necessary if high performance is key, but is more sensitive to interference.

•Efficiency: FHSS can provide up to four times more network capacity than DSSS. In the 2.4 GHz band, the maximum number of non-overlapping 2 Mbps DSSS channels is three (for a total capacity of 6 Mbps).

•Mobility: FHSS products provide better mobility, are smaller, lighter, and consume less power. Unlike DSSS, FHSS incorporates roaming without sacrificing throughput and scalability.

•Overlapping: This is a form of non-malicious interference caused by stray external radio emissions overlapping the network signals. DSSS networks are susceptible to overlapping, but FHSS networks can simply "hop around". FHSS products spend only milliseconds at each frequency. DSSS is not frequency agile. Products using DSSS are set at stationary, preselected frequencies and cannot avoid this interference.

•Immunity from Multipath Interference: Multipath interference is caused when signals bounce off of walls, doors, or other objects so that signals arrive at the destination at different times. This problem is automatically avoided by FHSS. FHSS simply hops to a different frequency that is not attenuated. DSSS is not capable of overcoming this effect.

1. Transmission Technology Evaluation

All transmission technologies are evaluated using the following equally weighted axis criteria and displayed in Table (2):

- Resilience against active attacks -
- Ease of hardware installation
- Resilience against interference/blockage

- Transmission speed
- Range between nodes
- Signal security

Axis		Rating	Meaning
a	Resilience against active attacks.	1	Possesses very little protection.
		2	Possesses some protection.
		3	Possesses moderate protection.
		4	Possesses good protection.
		5	Possesses complete protection.
b	Ease of hardware installation	1	Very difficult; contractor installation is required.
		2	Difficult; experienced personnel can accomplish.
		3	Moderately difficult; some experience required.
		4	Easy; experience helpful, but not required.
		5	Very easy; no experience required.
c	Resilience against interference/blockage.	1	Interference cannot be avoided.
		2	Difficult to avoid interference.
		3	Interference avoidable with some installed precautions.
		4	Some interference problems, but are avoidable.
		5	Has no interference problems.
d	Transmission speed.	1	Very slow.
		2	Slow.
		3	Moderately fast.
		4	Fast.
		5	Extremely fast.
e	Range between nodes.	1	Very poor; must be within a few feet of the AP.
		2	Poor; must be within same room.
		3	Average; AP's can be in adjacent rooms.
		4	Good; must be within same building.
		5	Very good; no range limitations when using directional antennas between buildings.
f	Signal security.	1	Unsecured; encryption/decryption does not prevent security intrusion.
		2	Poor; encryption/decryption may prevent security intrusion.
		3	Average; encryption/decryption prevents security intrusion.
		4	Secure; signal is difficult to break, but encryption/decryption is advised.
		5	Completely Secure; encryption/decryption is not required.

Table 2: Transmission Technology Axis Criteria

Each Technology is evaluated in Table (3) and results graphically displayed in Figures 22 and 23.

Technology	Axis	Rating	Meaning
Narrowband Microwave	a	3	Is susceptible to eavesdropping and denial of service.
	b	2	Professional installation necessary for FCC compliance.
	c	3	Interference avoidable with FCC licensing.
	d	5	Is a high speed radio frequency transmission.
	e	5	Is designed for use between buildings.
	f	3	Encrypted signal is mixed with the carrier frequency.
Infrared	a	4	Attacks must be initiated within the same room.
	b	5	Ad hoc configurations are installed using COTS products.
	c	2	Blockage is unavoidable.
	d	5	Very fast: 50 Mbps.
	e	1	Range is limited to three feet.
	f	1	Signal is not encrypted
FHSS	a	4	Is susceptible to physical denial of service.
	b	4	Requires basic installation skills. Algorithms and FCC requirements are pre-programmed.
	c	5	Can hop around interference.
	d	4	Uses radio frequencies at 2 Mbps.
	e	4	Must be within same building; range depends upon transmitter power.
	f	5	Hopping algorithms can be kept secret.
DSSS	a	3	Susceptible to all forms of attack, but its code is easier to break than FHSS algorithms.
	b	4	Requires basic installation skills. Bit codes and FCC requirements are pre-installed.
	c	3	Operates on pre-set frequency; susceptible to malicious transmitters.
	d	4	Maximum 8 Mbps if using expensive "top-of-the-line" equipment.
	e	4	Must be within same building; range depends upon transmitter power.
	f	4	Bit codes can be kept secret, supplementary encryption is advised.

Table 3: Transmission Technology Evaluation

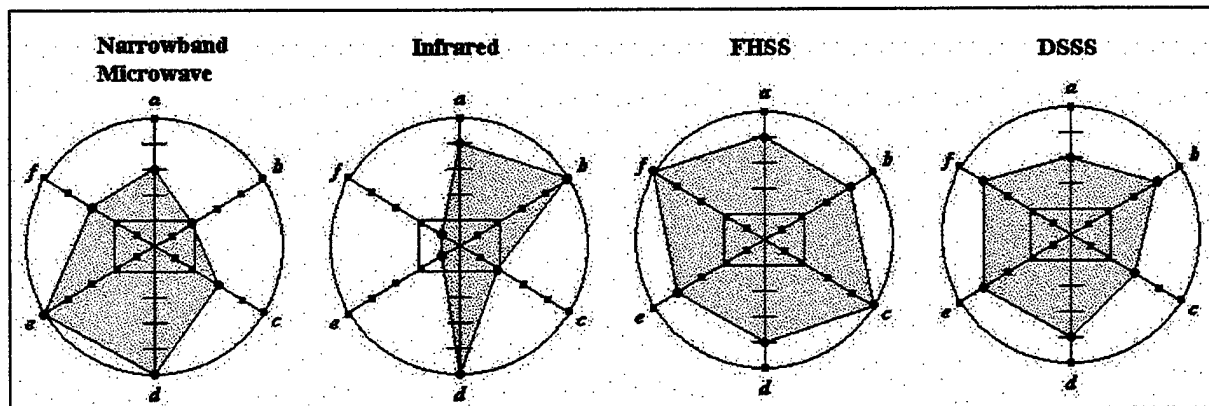


Figure 22: Technology Evaluation

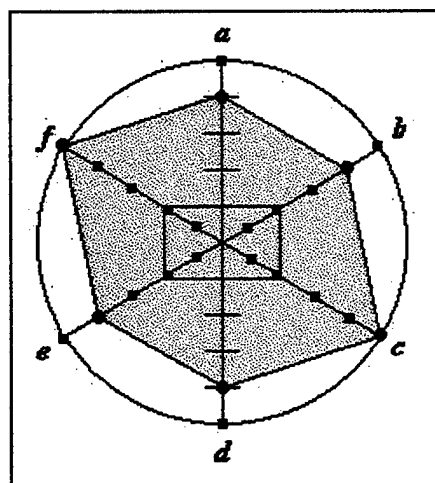


Figure 23: Best Technology (FHSS)

2. Best Technology Analysis

Both spread spectrum methods carry large volumes of data, but FHSS is superior. It is scaleable, mobile, secure, can accommodate overlapping networks, and is resistant to interference. FHSS is the best technology for 2.4 GHz wireless networks.

B. TOPOLOGIES

Multiple topologies have been discussed and are all acceptable networking architectures. Deciding *which* to use is dependent upon *how* the topology will be used. Evaluating each topology under generic conditions will determine the best model.

1. Topology Evaluation

Wireless topologies are evaluated using the same axis criteria as defined for transmission technologies with the exception of axis “d”. Criteria for transmission technologies axes “a” through “c” and “e” through “f” are directly related to wireless topologies while axis “d” criteria is not. Centrally shared resources are evaluated on this axis as defined in Table (4):

Axis	Rating	Meaning
d Use of Centrally Shared Resources	1	No access to centrally shared resources.
	2	Access to non-centrally shared resources.
	3	Access to shared resources, but not continuous.
	4	Access to shared resources, but not interactive.
	5	Continuous, interactive access to centrally shared resources.

Table 4: Axis “d” Criteria For Topology Evaluation

Each topology is evaluated in Table (5) and results graphically displayed in Figures 24 and 25.

Topology	Axis	Rating	Meaning
Ad Hoc (without centralized control)	a	1	Possesses no MAC controls; susceptible to active attacks.
	b	5	Any computer can be added to the network.
	c	2	Has no wired protections within the network.
	d	1	Has no access to centrally stored resources.
	e	2	Is susceptible to physical blockage (walls).
	f	1	Possesses no network firewall nor secure backbone.
Ad Hoc (with centralized control)	a	1	Possesses no MAC controls; susceptible to active attacks.
	b	5	Any computer can be added to the network.
	c	2	Has no wired protections within the network.
	d	3	Has access to one BS.
	e	3	Is range restrictive, but the BS recognizes node drift.
	f	1	Possesses no network firewall nor secure backbone.
Cellular	a	3	Security; protective measures built into wired segments.
	b	4	Access to the wired BS requires configuration.
	c	4	Mobile unit can be handed off to another cell if blocked..
	d	4	Access to one BS at a time; simultaneously access to multiple mobile units.
	e	4	Communication with remote BS via wired segments.
	f	3	Encryption/decryption required on wired segments.
Non- Cellular	a	3	Protective measures built into wired segments.
	b	4	Access to the wired BS requires configuration.
	c	2	Interference/blockage is easy at the wireless segments.
	d	4	Simultaneous access to multiple BSs, but does not know which mobile stations are associated with these BSs.
	e	3	Communication with remote BSs via wired segments, but drift may occur.
	f	3	Encryption/decryption required on wired segments.
Personal Area Networks	a	4	Attack must be initiated within the same room.
	b	3	Configuration needed between mobile units and peripherals.
	c	2	Blockage is unavoidable.
	d	3	Has access to non-centrally shared peripherals.
	e	1	Range is limited to three feet using inexpensive equipment.
	f	2	Doesn't have a protected wire backbone.

Table 5: Topology Evaluation

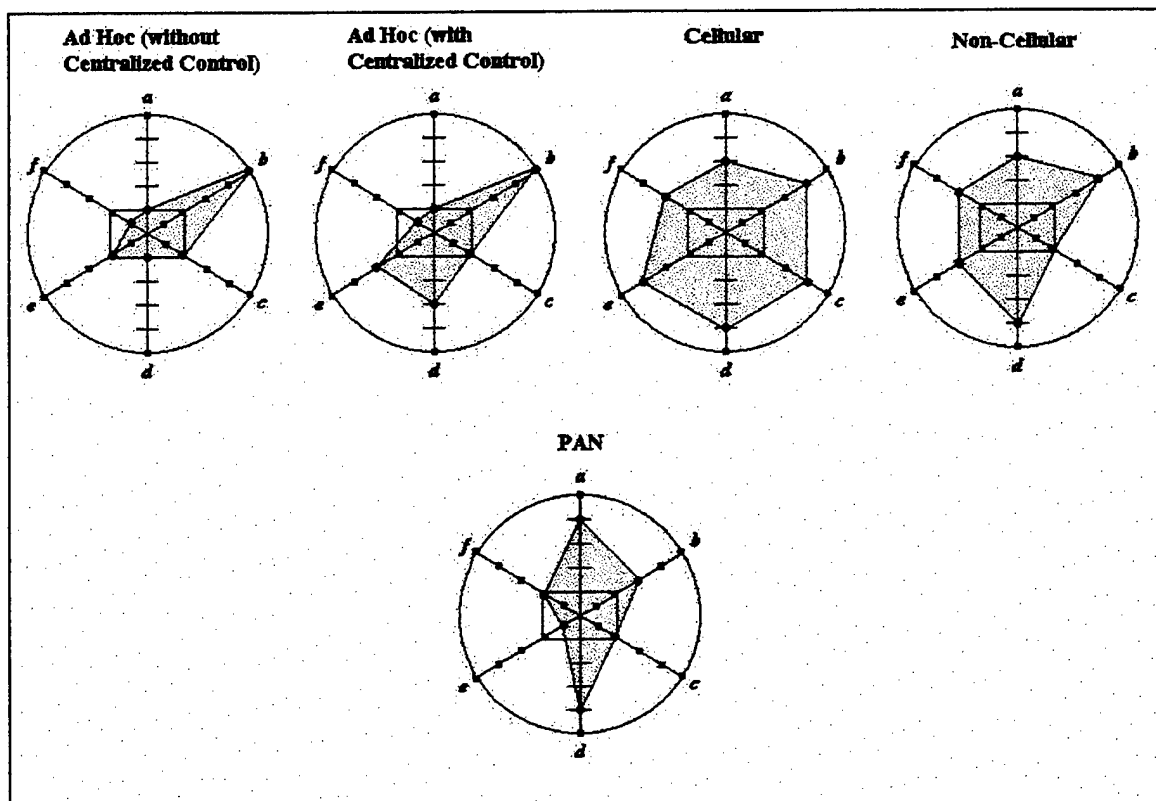


Figure 24: Topology Evaluation

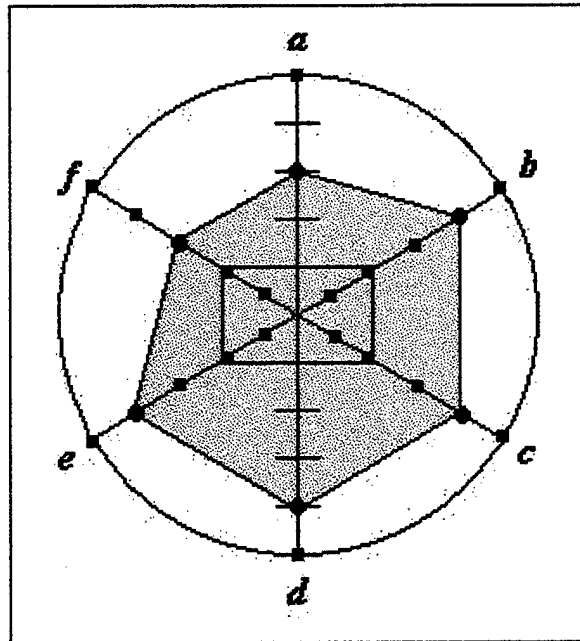


Figure 25: Best Topology (Cellular)

2. Best Topology Analysis

Cellular topologies are the best for general usage. It's coverage area is adequate for both small and large LANs and network resources are shared.

C. VENDOR TOPOLOGIES

Commercial products are diverse. Some are specifically designed for small offices while others provide signal transmission from building-to-building. Each is evaluated using methods similar to those used to analyze technologies and architectural topologies.

1. Vendor Topology Evaluation

Evaluation is limited to vendors that use FHSS with Cellular-based topologies thus eliminating products not suitable for DoD. Axis criteria for "b" and "d" are identical to those used for the technology analysis. Criteria for remaining axes are defined in Table (6).

	Axis	Rating	Meaning
a	Compliance with IEEE 802.11/HIPERLAN	1	Not compliant with known standards.
		2	Compliant with standards other than IEEE 802.11/HIPERLAN.
		3	Compliant with HIPERLAN only.
		4	Compliant with IEEE 802.11 only.
		5	IEEE 802.11 and HIPERLAN compliant.
c	System Management	1	Very difficult; requires continual contractor maintenance.
		2	Difficult; requires scheduled contractor maintenance.
		3	Moderate; requires some maintenance experience.
		4	Easy; maintenance experience not required.
		5	"Hands-off"; system maintains itself during normal operation.
e	Scalability/expandability	1	Not expandable after installation.
		2	Expandable, but very limited.
		3	Expandable, but limited.
		4	Easily expandable.
		5	Unlimited expandability.
f	Compatibility	1	Not compatible with any other vendor product.
		2	Compatibility limited to unacceptable vendor products (IR, Narrowband).
		3	Compatible with some vendor products.
		4	Compatible with most acceptable vendor products.
		5	Compatible with all analyzed products.

Table 6: Vendor Topology Axis Criteria

Each vendor topology is evaluated (Table 7) and results graphically displayed in Figures 26 and 27.

Vendor Topology	Axis	Rating	Meaning
AIR-VO	a	5	Is IEEE 802.11 and HIPERLAN compliant.
	b	3	Hardware installation difficulty is moderate, but software requires vendor configuration.
	c	3	Possesses multiple software peripherals requiring experienced management.
	d	3	Provides for adequate bit rate at 2 Mbps.
	e	4	Easily expandable using software/hardware from same manufacturer.
	f	4	Can be used in conjunction with other manufacturers, but is not specifically designed for this.
Jaguar	a	5	Is IEEE 802.11 and HIPERLAN compliant.
	b	5	Installation is "plug-and-play".
	c	4	Some training involved for AP hopping pattern configuration.
	d	4	Provides a good bit rate at 3.2 Mbps.
	e	4	Expandable to 62 users with 15 overlapping cells.
	f	4	Can be used in conjunction with other manufacturers, but is not specifically designed for this.
WaveLyNX BR132	a	5	Is IEEE 802.11 and HIPERLAN compliant.
	b	3	Directional antenna installation required.
	c	5	Settings are pre-configured.
	d	4	Provides a good bit rate at 3.2 Mbps.
	e	3	Limited to bridge routing between buildings.
	f	4	Can be used in conjunction with other WLAN manufacturers.
NetWeaver	a	5	Is IEEE 802.11 and HIPERLAN compliant.
	b	3	Directional antenna installation and configuration required.
	c	3	Some post installation maintenance required.
	d	4	Provides a good bit rate at 3.2 Mbps.
	e	5	Unlimited.
	f	5	Is designed for compatibility with other vendors.

Table 7: Vendor Topology Evaluation

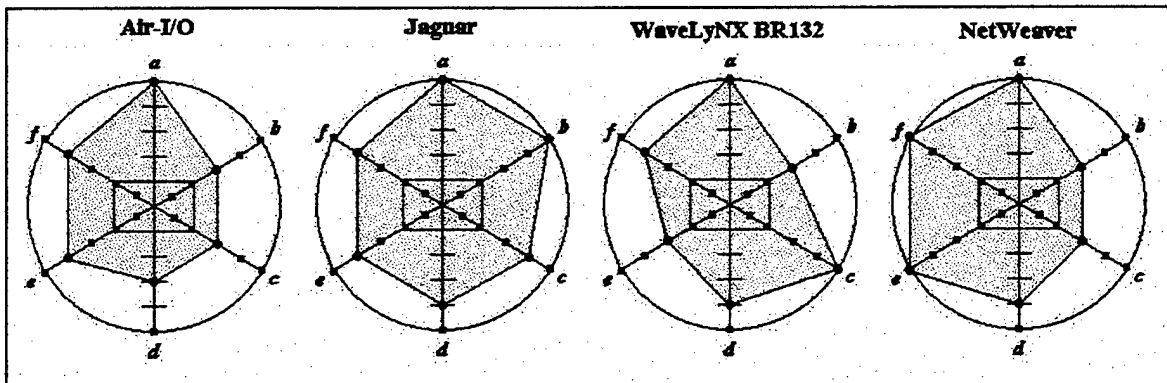


Figure 26: Vendor Topology Evaluation

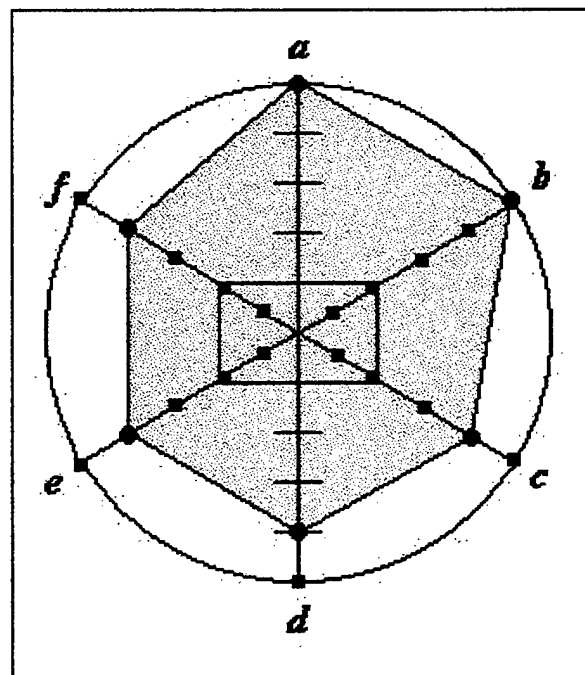


Figure 27: Best Vendor Topology (Jaguar)

2. Best Vendor Topology Analysis

Each vendor topology has its strengths and weaknesses and can be used to meet specific needs, but Jaguar is the most balanced. It offers flexibility, expandability, and vendor compatibility.

D. WLAN CASE STUDY: WIRED SEGMENT REPLACEMENT

This case study evaluates security implications of incorporating wireless technology in a standard wired LAN at the Naval Postgraduate School (NPS) in Monterey, CA. The LANs physical and logical organization are discussed, then replacement of wired links with wireless is examined. The security effects of each substitution are investigated.

Figure (28) shows the NPS Token Ring LAN architecture located in a classroom at Ingersoll Hall. It is hard wired to the larger campus backbone that provides both Internet and intercampus LAN access. There is a firewall between the campus backbone and the Internet, but not between the backbone and the LAN. Each LAN client runs Windows NT and communicates with the server and other users via Multistation Access Units (MAUs). These client computers are assigned names (TN31, TN32, TN33, etc...) for physical identification during routine maintenance and repair by System Administrators. Administration is managed at the server, but a System Administrator can login using his account access from any LAN client. Most applications are pre-loaded onto the individual terminals, but some are centrally stored on the server.

Logical LAN organization uses domains to manage permission databases, groups for assigning broad sets of permissions to multiple users, and user accounts to control security at each client. The domain is a logical arrangement of LAN hardware resources referenced by a specific name. It provides a single security permissions database used by all clients attached to it. Ingersoll's LAN is a part of the 'Systems Management' domain. Groups are security entities within the domain that offer broad sets of permissions to users assigned to it. It allows System Administrators to control access to a large collection of users rather than assigning permissions to individual users. Users can be simultaneously assigned to more than one group. User accounts are referenced by user names and contain passwords, permissions, group associations, and user preferences.

The physical and logical LAN organization are tied together when an authorized user logs into the system. The user can login to the network from any client attached to

the Systems Management domain by providing their user name and password. This account information is passed to the server which authenticates the user. Once authenticated, the user becomes a part of the network and can use its resources. During this process users will see the domain that they are logging into, but their group association is transparent to them and pre-assigned by system administrators. The server also has an optional guest account. This allows general access to resources and can only be enabled from an administrator account. Ingersoll's LAN administrators have disabled this option, because it allows anyone to login to the network leaving the system vulnerable to attack by malicious users.

While attached to the network, users can share each others resources using the file transfer protocol (FTP). User "A" can make his workstation the FTP server while user "B" becomes the FTP client. Once "A" accepts "B" as an authorized client, the FTP application allows "B" to see and download files from "A".

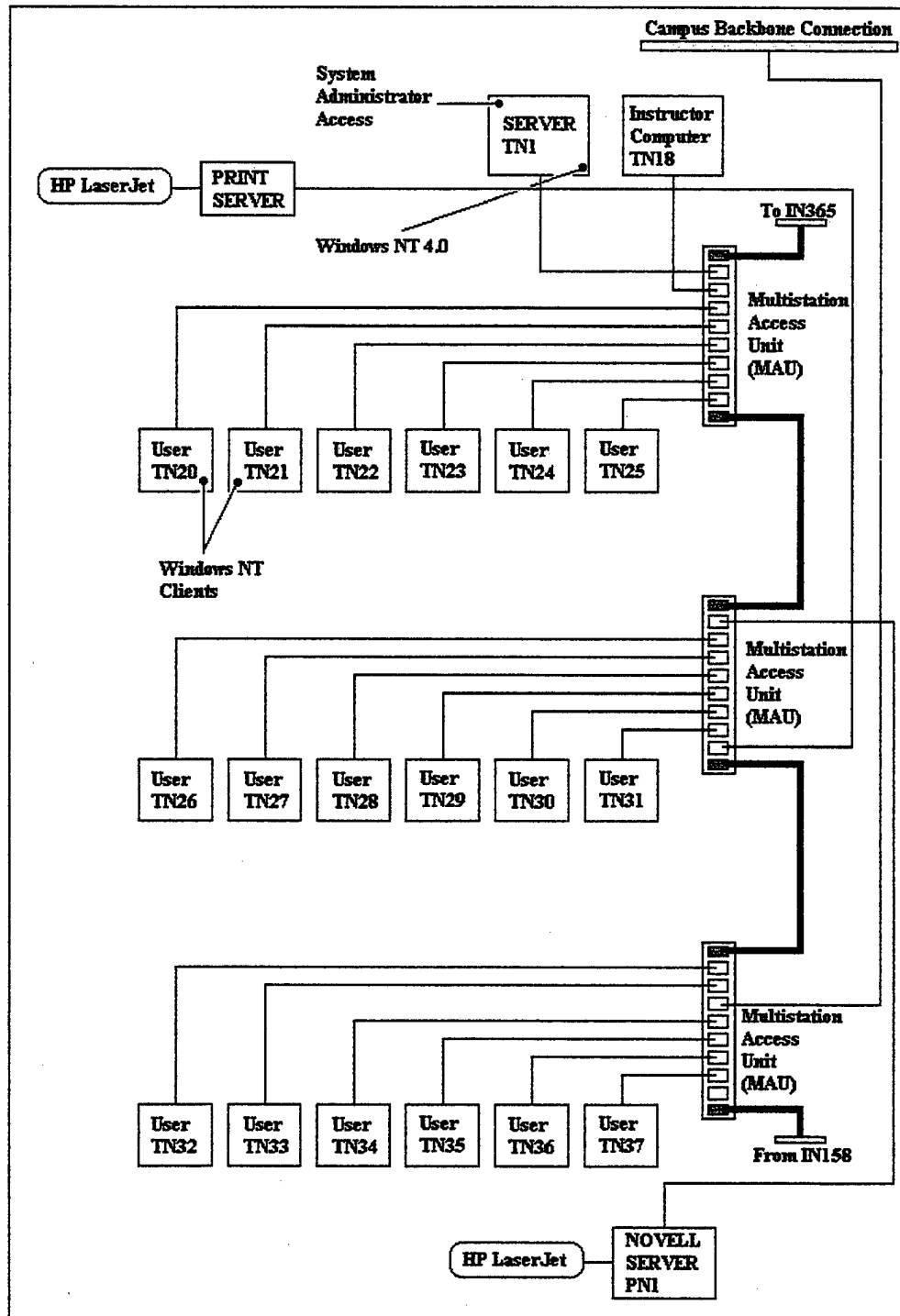


Figure 28: Ingersoll 224 Token Ring LAN

Maintaining user mobility while retaining LAN connectivity is desired. Replacing wired LAN segments with wireless provides many alternatives for achieving

this mobility. Some options provide diversity as to where different portions of the LAN can be installed while maintaining a wireless connection to the network. Other options provide physical user mobility to the client. Eventually, although not presented here, users will be able to operate within one WLAN, logoff when complete, physically move their client to another WLAN in another location, and login without reconfiguring their computer. The user needs only to specify the new domain from a drop-down menu and login using their account information. The RF transmission between the laptop and network AP would be decoded at the AP with the account information forwarded to the server for verification. With these options in mind, administrators may choose to deviate from standard wireless network architectures and create wired/wireless LAN hybrids. Possible wireless segmentation is discussed.

1. Wireless Between User and Multistation Access Unit

The replacement of wires between users and a MAU by wireless connections is evaluated first. The advantage of this architecture is that it permits some or all users to roam outside of the classroom while remaining connected. Figures (29) and (30) show this architecture.

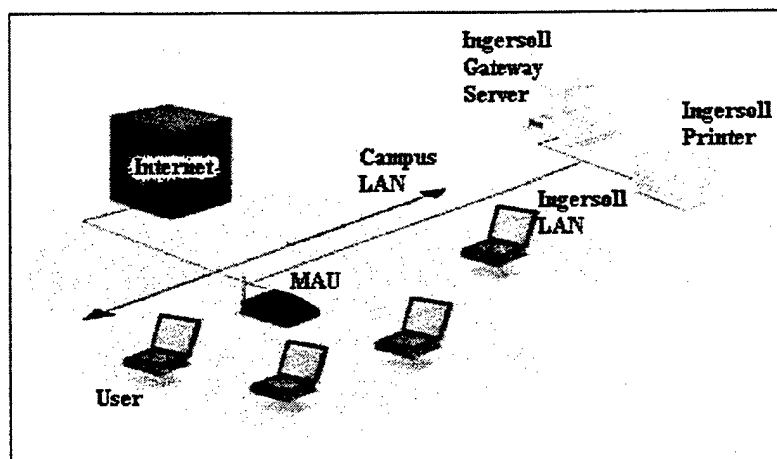


Figure 29: Hard Wired LAN With Wireless Users

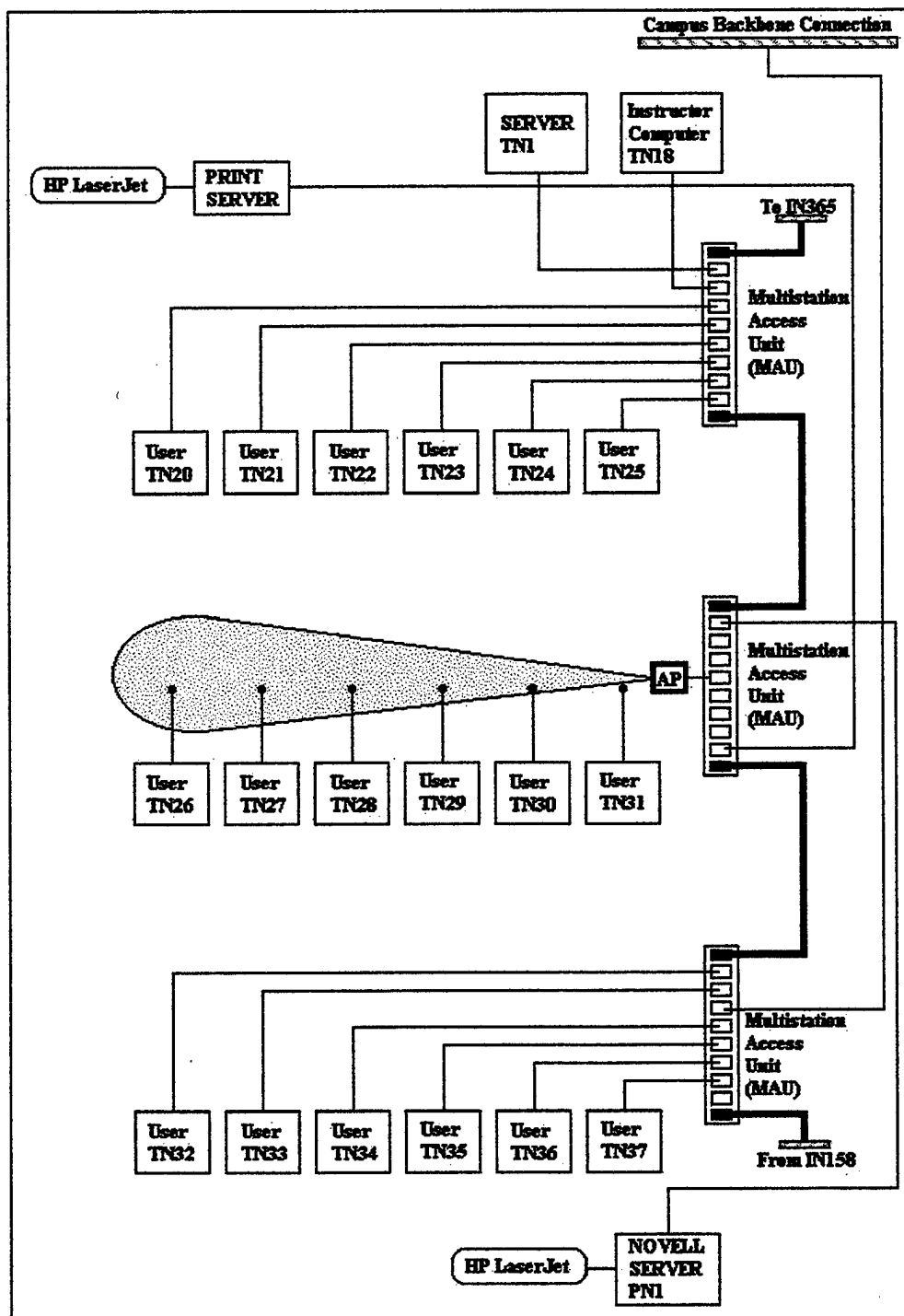


Figure 30: Wireless Between User and Multistation Access Unit

When logging into the network the user ensures that his drop down menu shows the domain name 'Systems Management'. After typing in his account information the user pushes "enter" and sends the data, via RF signal, to the receiving AP. The AP translates the signal back into binary code and forwards the request to the server. The server acknowledges receipt of the data, and either accepts or rejects the user. If authorized, the user joins the network. User mobility is maintained without weakening access security. All communications between mobile units and network resources are still passed through MAUs. This configuration also uses fewer MAU ports, thus freeing them for other devices.

2. Wireless Between Servers and Multistation Access Units

A topology in which wired connections between the server and MAUs are replaced with wireless technology is evaluated next. The advantage for this topology is that it allows a MAU and its attached clients to be placed in a room separate from the server while keeping a connection to the network. Figures (31) and (32) show this architecture.

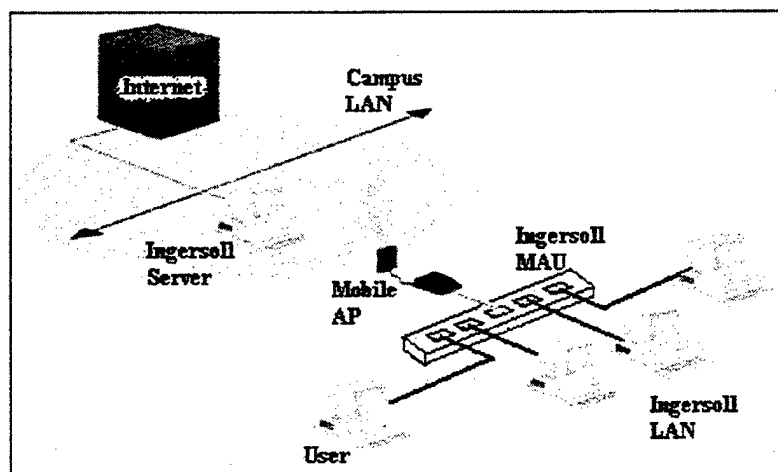


Figure 31: Hard Wired LAN With Wireless Connection Between Server and MAU

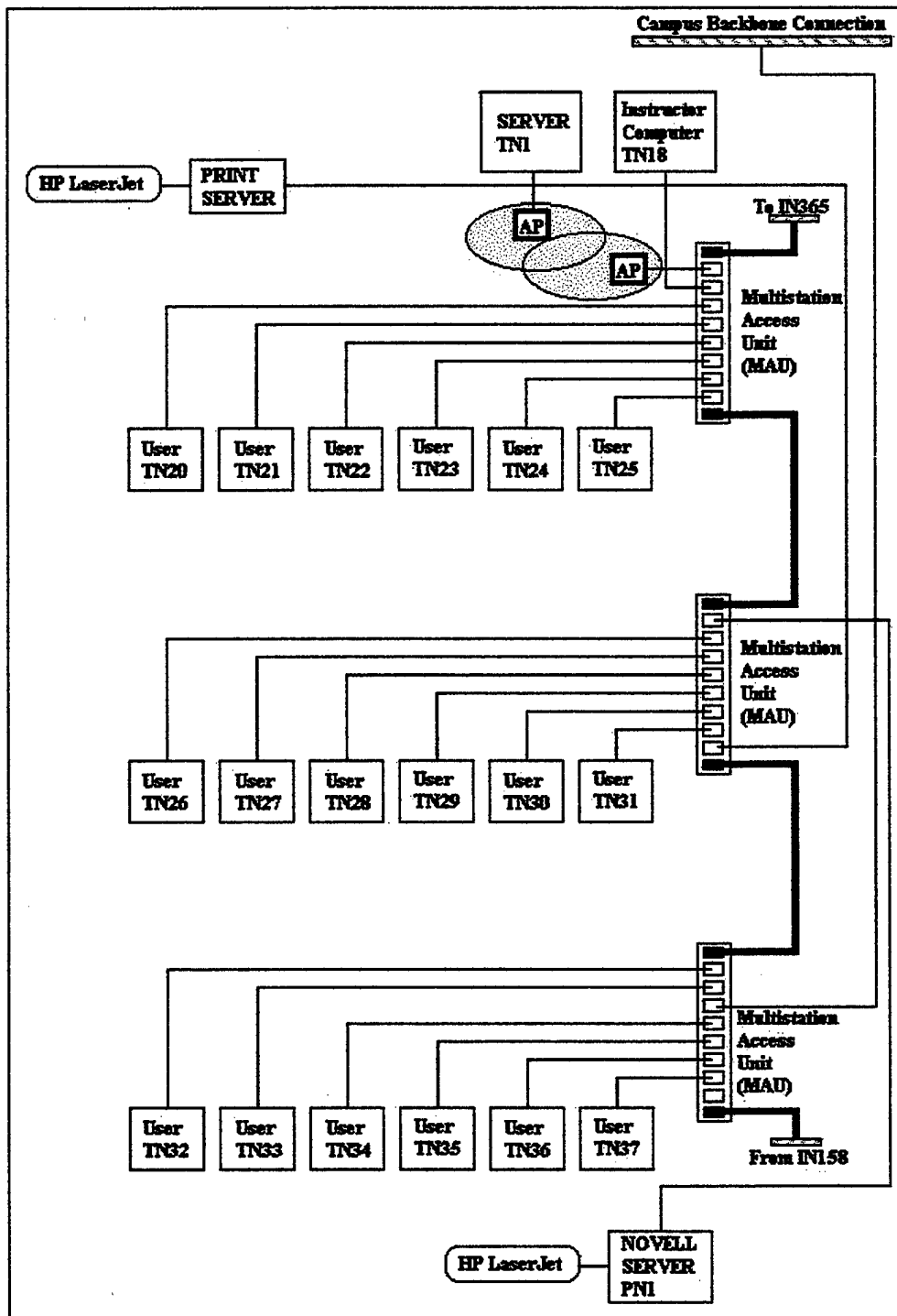


Figure 32: Wireless Between Server and Multistation Access Units

As in the previous example, security is not compromised, because access controls are still in place. Users must still login to the server and be granted access prior to entering the network.

3. Wireless Between Multistation Access Units

The benefits achieved by replacing wired connections between MAUs are few, but notable. Wireless connections between MAUs do not increase client physical mobility, but offer user virtual mobility. Connected users can logout, physically move to a different client in a different room, and login again resuming their connection to the network. Hardware expense is also saved, because wires don't need to be installed between MAUs. User login procedures remain the same. Figure (33) shows this schematic.

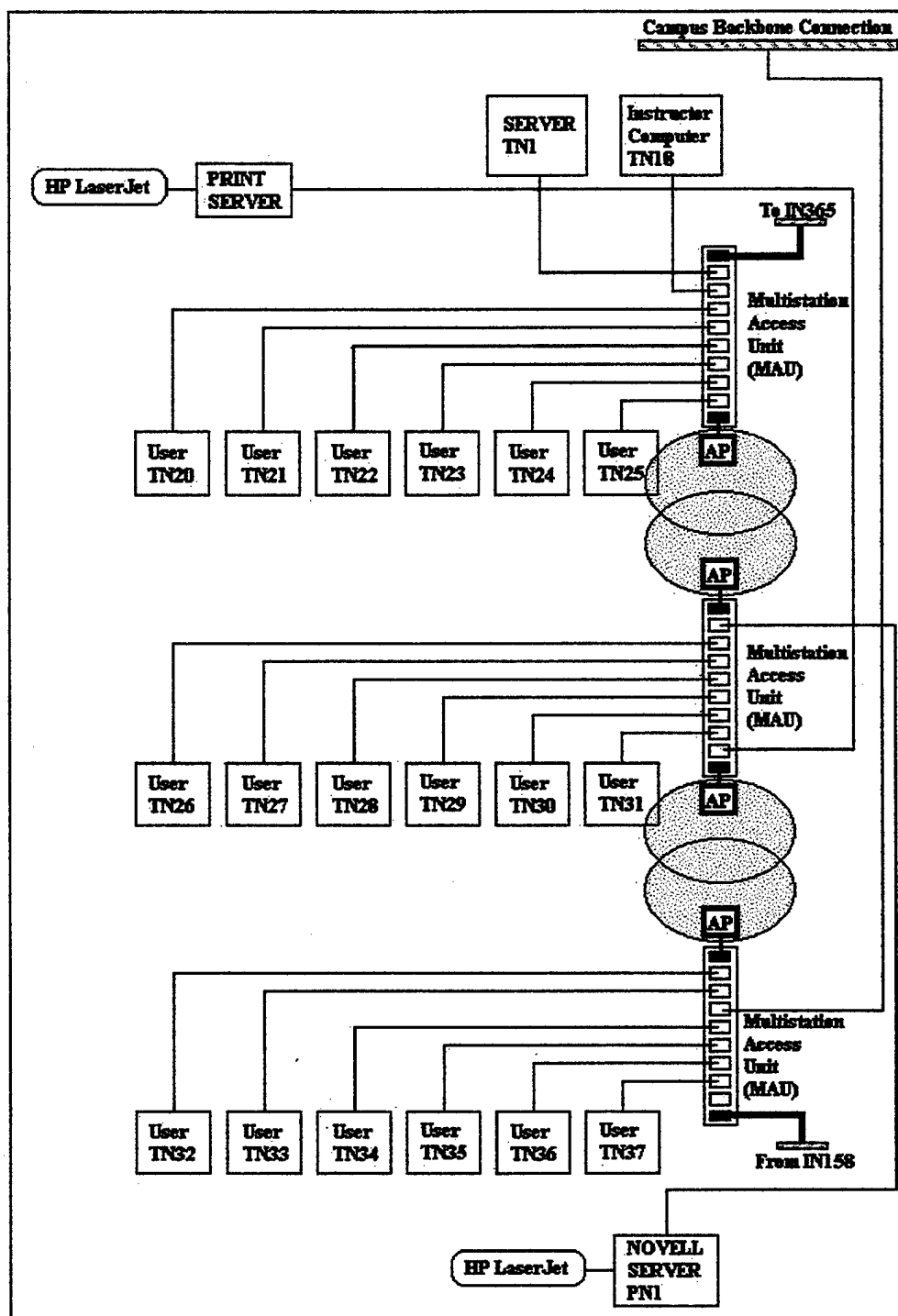


Figure 33: Wireless Between Multistation Access Units

4. Wireless Between Backbone and Ingersoll LAN

Replacing the connection between the LAN and campus backbone with directional wireless antennas is evaluated next. There are cost savings in this case, because LANs are connected to the backbone without purchasing and installing wire. The firewall is still located between the backbone and the Internet, so overall security is not degraded. Access within the LAN is still handled by the server. One concern is the RF transmission being “in the open”. An attack in the preceding examples have to overcome physical obstructions such as walls and doors. The LAN-to-backbone wireless connection puts the signal outside of the building thus making it more susceptible to exploitation or interference, because an attacker need not worry about penetrating the building structure. Figures (34) and (35) show this architecture.

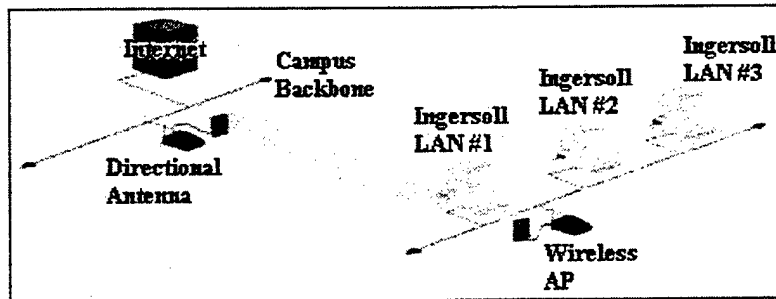


Figure 34: Hard Wired LAN With Wireless Connection to Campus Backbone

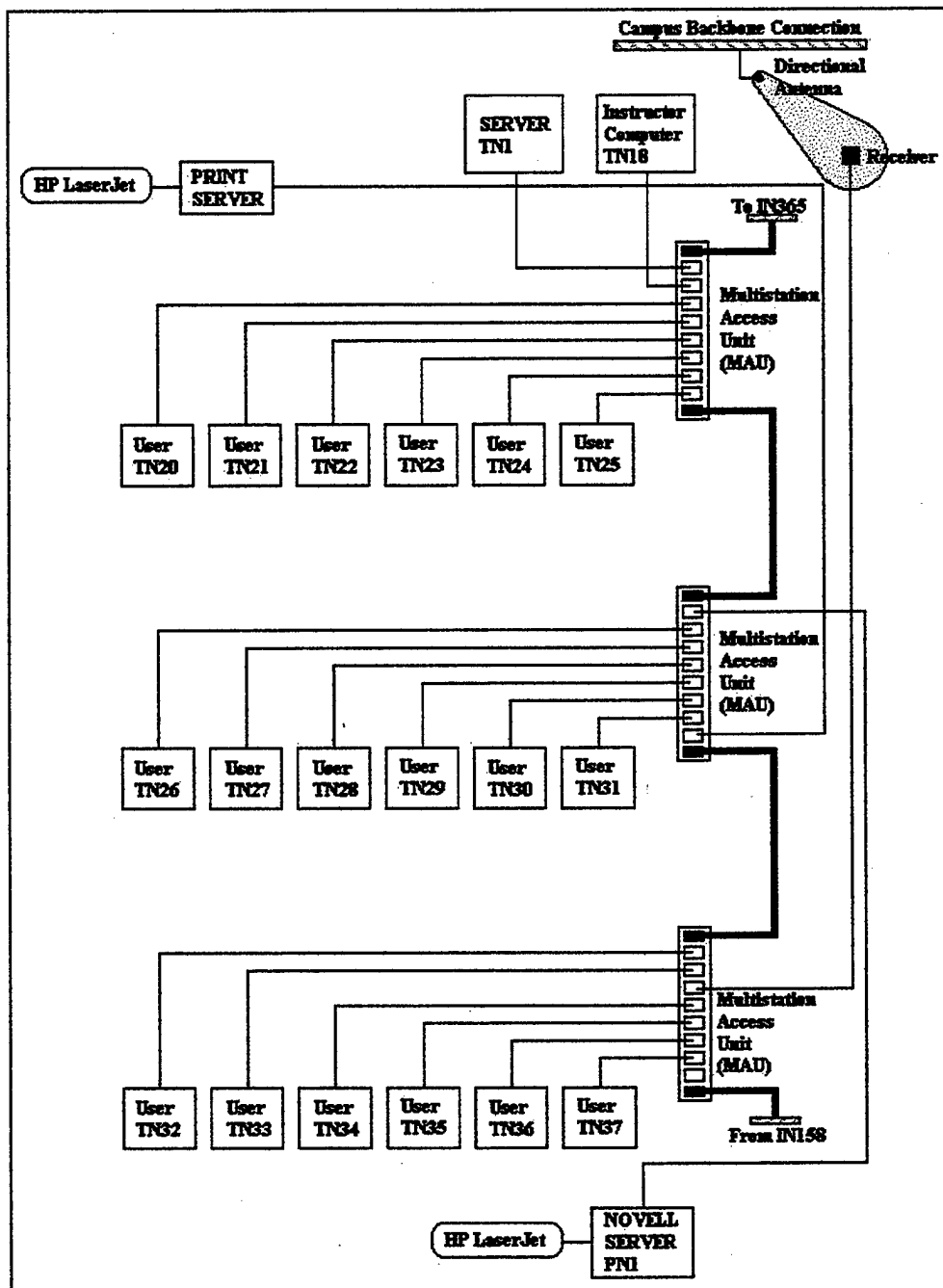


Figure 35: Wireless Between Backbone and Ingersoll LAN

5. Summary

Each configuration has its strengths and weaknesses. There is no single solution that is applicable to all WLANs. Administrators must first determine their requirements and then decide which segments to replace. For example, if all users are using desktop

computers in the same room, it makes no sense to install wireless segments between these users and the MAUs. Their computers would become theoretically "mobile", but their physical size and weight would keep them stationary. After determining LAN requirements, an administrator can choose from previously mentioned vendor topologies or develop a hybrid of his own.

E. WIRELESS LAN CASE STUDY: WIRELESS SEGMENT ATTACKS

Wireless segment replacement has its advantages, but it can also make the network vulnerable to attack. FHSS is indiscernible to unauthorized receivers, but a knowledgeable attacker who knows the hopping algorithm can decode the received signal. Additionally, an attacker can still disrupt the network without knowing any algorithms. In either case, the level of vulnerability depends on the network configuration. The following are methods that an attacker can use to exploit wireless segmentation.

1. By-passing Access Controls; Frequency Hopping Algorithm Known

Windows NT 4.0 user groups control access to specific network resources. Figure (36) shows a poorly placed AP between the server and an extended resource such as a database located on another machine. The server authenticates users prior to granting access, but an attacking transceiver can transmit into the signal "cloud" and gain access to the unprotected resource. The attacker can then enter the server spoofing the extended resource. If the server trusts the intruder, the attacker can control all services provided by the server and manipulate the network. Users can be fooled into sharing sensitive or classified information and may also unknowingly log-in directly to the attackers system via the server. Other unauthorized actions include:

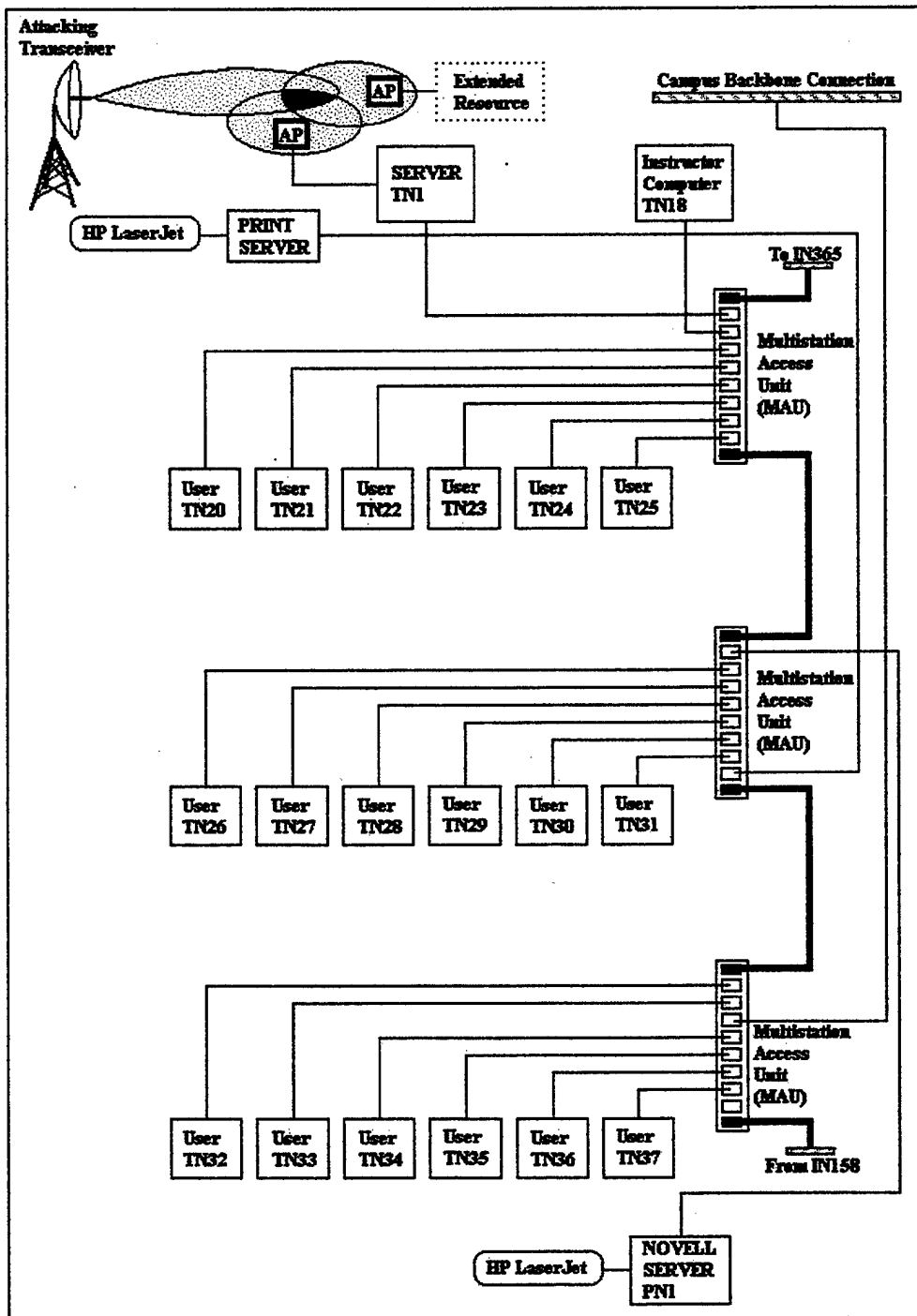


Figure 36: By-passing Access Controls; Frequency Hopping algorithm Known

a. Resource Exploitation

The attacker can obtain information from the server and use it to his advantage. He can download any personal information about users with authorized network access.

b. Falsifying Information

The attacker can transmit false information to authorized network users. This damages resource integrity and can lead to cascading problems as users apply or pass this information to other users.

c. User Access Data

The attacker can acquire group access data thereby gaining knowledge of which users have the fewest access restrictions. This helps the attacker focus future exploitation on specific users who have higher network privileges.

2. Bypassing the Firewall; Frequency Hopping Algorithm Known

Figure (37) shows a directional antenna placed between Ingersoll's LAN and the campus backbone. Knowing the frequency hopping algorithms allows an unauthorized transceiver to intercept data transmissions between the backbone and LAN receiver. This effectively allows the attacker to bypass the firewall. Once inside the backbone, the attacker can potentially access all network servers within NPS. It can also receive and send data through all connections accessed by Ingersoll's LAN.

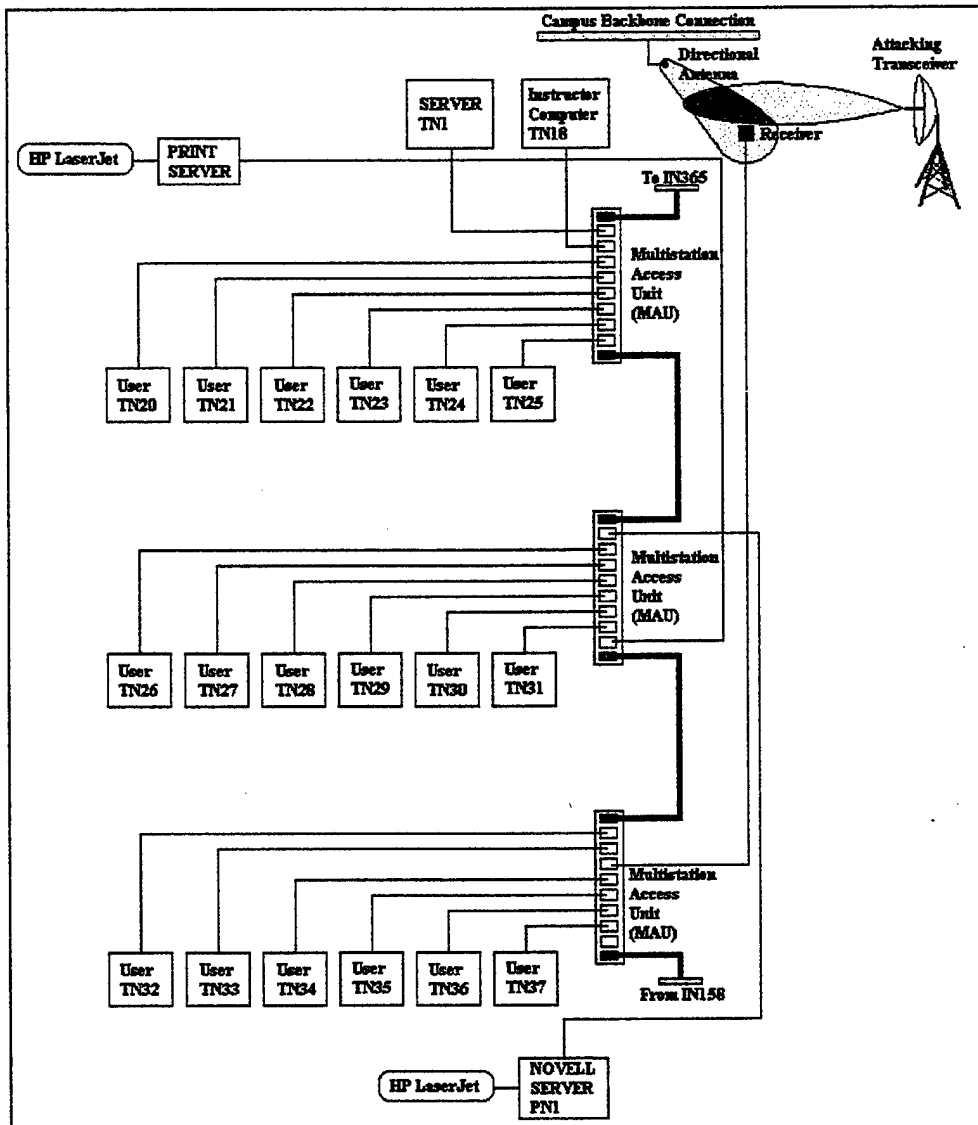


Figure 37: Intrusion Inside the Firewall; Frequency Hopping Algorithm Known

3. Direct Connection to Wireless Users; Frequency Hopping Algorithm Known

Figure (38) shows an unauthorized transceiver gaining direct access to wireless network users while circumventing both firewall and server access protection. This allows the attacker communication with users and possibly IP spoofing to implement a transitive trust attack. Using another user's IP address the attacker fools an authorized user into logging into the attacking system by luring the victim into believing the attacker

is the server. This method also allows the attacker to trick the server into thinking that the intruder is a valid user. These attacks are initiated using a couple of techniques.

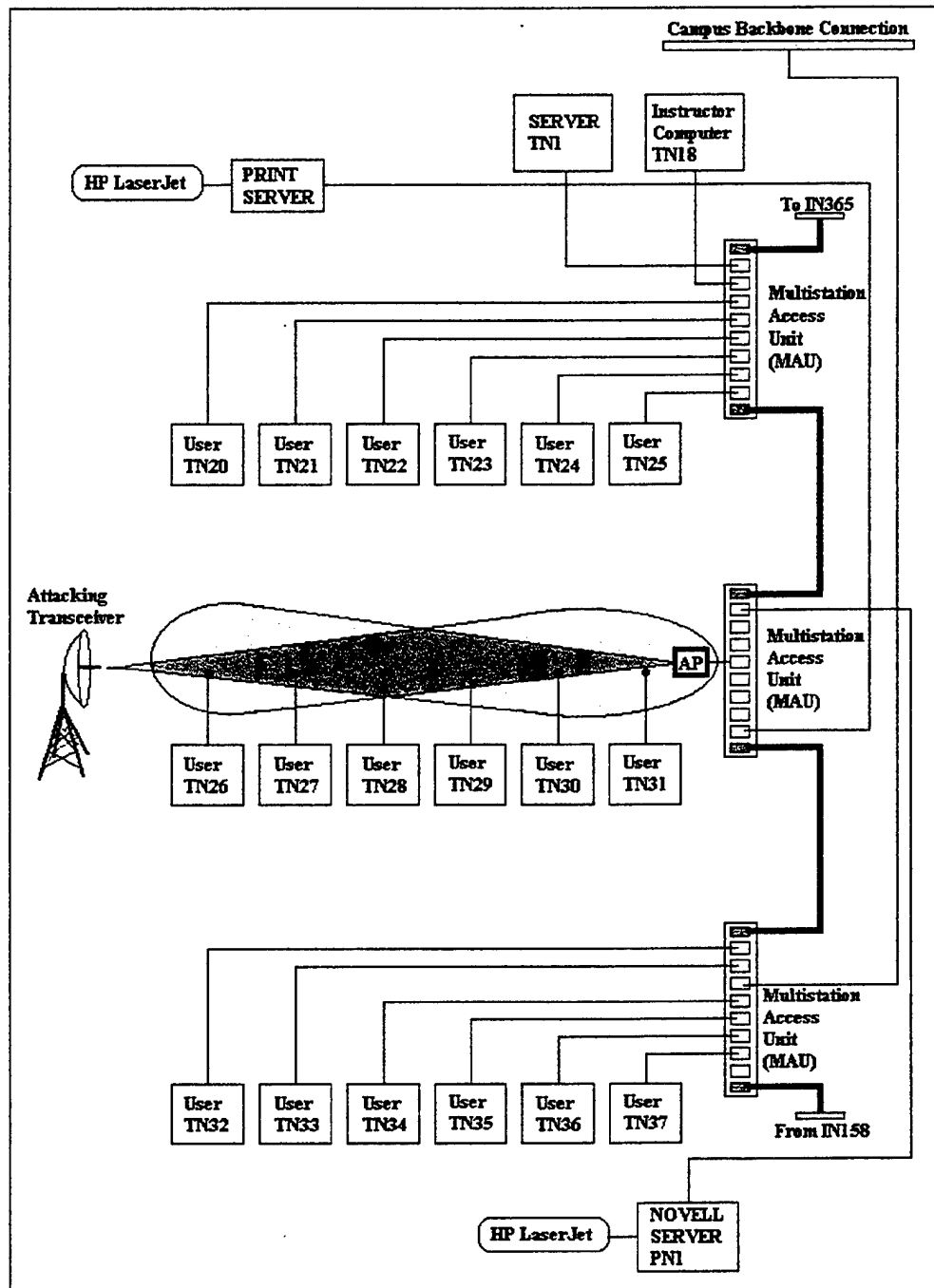


Figure 38: Direct Connection to Wireless Users; Frequency Hopping Algorithm Known

a. *Direct User Connection*

This method allows direct connection to users by “dialing” into their machines. With a spoofed IP address, the attacker sends a signal directly to the user requesting an FTP connection. After the unsuspecting user accepts the intruder as a fellow authorized user, the attacker has control of the user’s files. Subsequently, the attacker can use the compromised machine to gain access to server resources posing as the victim user.

b. *Indirect User Connection*

This requires the attacker to gain access to the server first and then communicate with a user while presenting himself as another valid network user. The initial RF signal is sent directly to the AP, is passed onto the server, and is accepted using a spoofed IP address. The attacker can then communicate with any network user. The valid user doesn’t suspect the intrusion because it believes the attacker to be valid.

**4. **IP Spoofing Between Multistation Access Units; Frequency Hopping
Algorithm Known****

Figure (39) shows an attack on transmissions between MAUs. This doesn’t provide direct RF access to users or servers, but allows manipulation of data being passed between LAN portions. With enough illegally confiscated data, the attacker can initiate a number of attacks posing as other users.

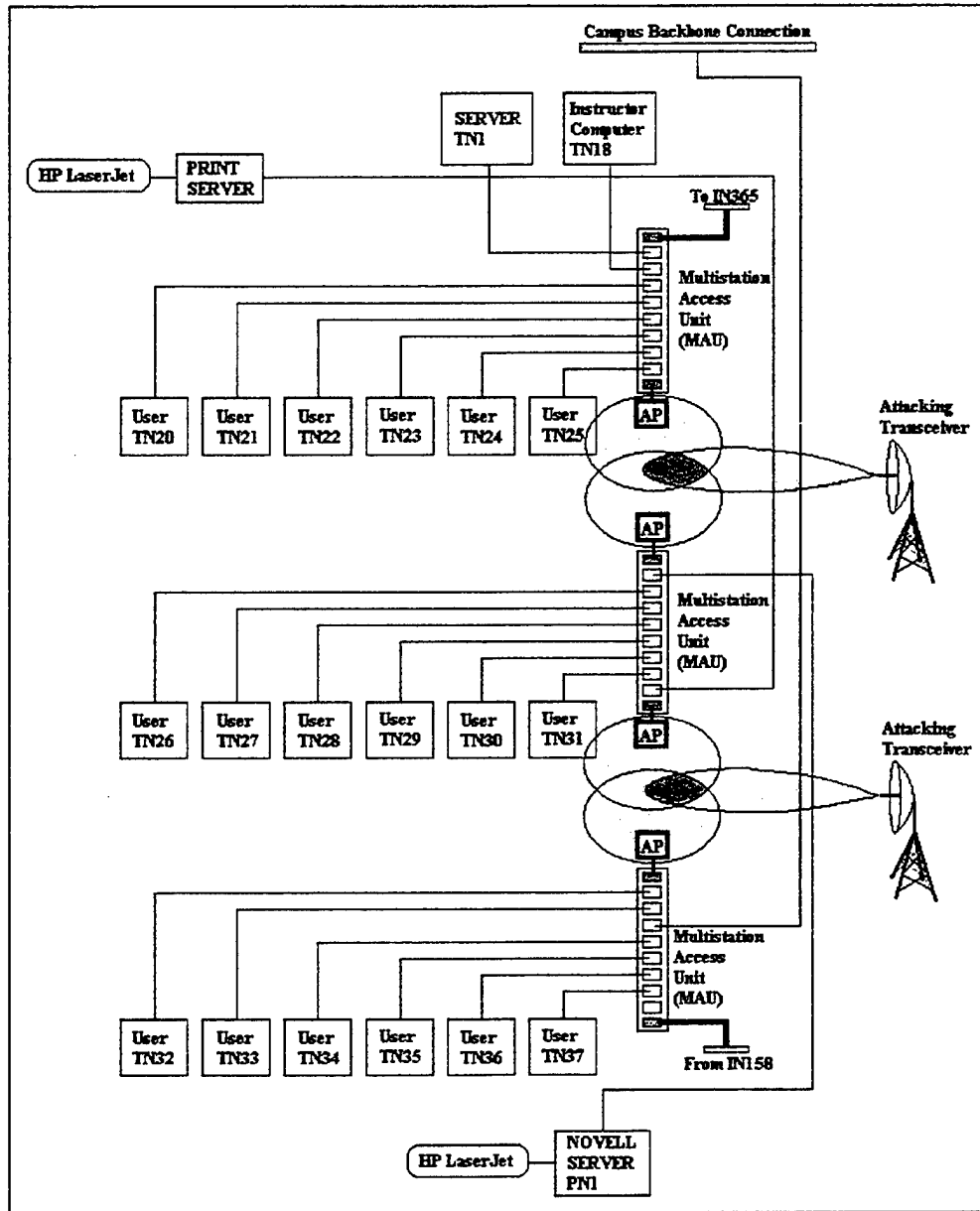


Figure 39: IP Spoofing Between MAUs; Frequency Hopping Algorithm Known

5. Denial of Service; Frequency Hopping Algorithm Not Known

Figure (40) shows transceivers attacking all wireless sections of the network. Without knowing the FHSS hopping algorithm, the attacks can transmit enough power to override authorized signals. This nullifies valid transmissions and renders the network physically useless for the duration of the attack.

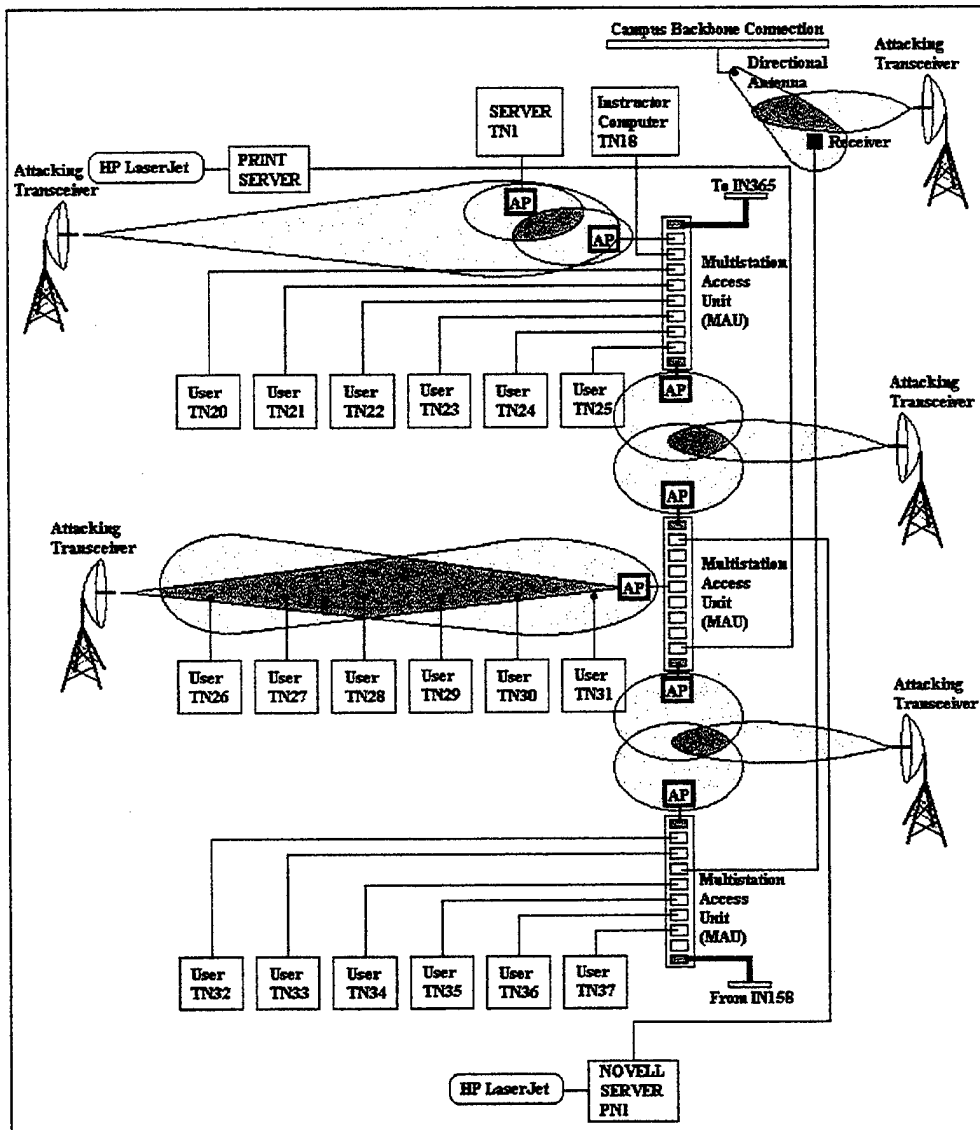


Figure 40: Denial Of Service; Frequency Hopping Algorithm Not Known

F. WIRELESS LAN CASE STUDY: DETECTING THE ATTACKER

The previous examples show how an attacker can exploit the network. Detecting these attacks requires diligence and an understanding of how the network is mapped. Using Windows NT 4.0 server manager a systems administrator can “see” all users who are online and which workstations they are using, but this doesn’t provide information about malicious attacks launched by wireless invaders from outside of the network. Two methods for detecting unauthorized wireless intrusions are: using software sniffers and

using hardware transmitter detectors. This section will provide a synopsis of possible ways to defeat attacks specific to wireless networks. It does not provide a survey of all tools available for this detection, but rather two possible technologies to combat such attacks.

1. Software Sniffers

Sniffers are more important to WLANs, because misuse of the network is easier. This is due to the fact that access to the transmission medium is not as physically controlled as it is in hard wired LANs. Intrusion detection, discussed in previous sections, uses software tools that look for irregular data packet transfers between nodes. This irregularity is determined by the type of attack being initiated. These applications may detect when an unauthorized user has hacked into the network. If the network sniffer detects an irregularly named user, then that user may be accessing the network in an unauthorized capacity. For example, users might be online using only three terminals, TN26, TN27, and BERTHA. Suppose that BERTHA is not a name assigned to any authorized workstation. The user may be using an authorized user name and password with an unauthorized workstation, or may have simply found a way to hack into the network using a spoofed user name and password. These conditions are the same for wired and wireless networks. The attacker must still access the LAN via an AP, so the network administrator can detect the intruder at this choke point. Then other methods specific to wireless can be employed to locate the attacking transmitter.

2. Hardware Detector Detectors

Locating an attacking transceiver can only begin after an ongoing attack has been detected. As described in the previous section, packet sniffing can be used to detect unauthorized activity on the LAN. To accomplish an attack the intruder has to be transmitting a signal into the LAN's AP. Devices are available that can track the intensity of and the direction from which a signal is generated. An attacker who is passively listening to data transmissions between mobile nodes and LAN APs can also be tracked. In order to receive and use an FHSS signal the attacker's receiver must be receiving the signal at the same frequencies that the carrier signals are using. Once captured, the attacking receiver decodes the signal into usable data with an internal oscillator that tunes to the received signal frequency. This oscillation causes leakage

current detectable using inexpensive tracking receivers. These receivers may be large and very sensitive or small and dedicated to picking up leakage current from very small coverage areas. Such receivers can be created using equipment purchased from any electronics store. Once this frequency leak is detected, the direction from whence the attack is emanating is determined and the intruder can be located. These leakage detection receivers have been used by television movie subscription companies for over 15 years to track unauthorized reception antennas mounted on homes and offices. They are not currently provided by makers of wireless products, but could be included in the arsenal of intrusion detection tools.

V. CONCLUSION

Wireless LANs will eventually be a common alternative to the wired LAN. Wireless networking is a rapidly emerging technology and security must be addressed as it is incorporated into new and existing networks. What are the unique properties of wireless LANs that might amplify existing LAN vulnerabilities or introduce new ones? This study began with the review of available technologies. Wireless transmission techniques, topologies, and vendor offerings were surveyed from a security perspective. This information was graphically displayed using Kiviat drawings to show symmetric comparisons of each analysis category. FHSS transmission technology, cellular topology, and the Jaguar product emerged as the best approaches available. These results were applied to a case study that examines network wired segment replacement options, wireless segment attacks, and methods to detect an attacker.

Future wireless networks should provide easy connectivity between authorized clients and the network with which they are associated. These systems must be built to be secure from the ground up. Pushing vulnerability mitigation to the final phases of development will leave security loopholes that are impossible to close. Hardware encryption/decryption devices are not used by most products, but software encryption exists in the form of transmission algorithms. Leakage current detectors, discussed in Chapter Four, should also be designed for WLAN system compatibility and then sold as an intrusion detection tool. This would alleviate problems associated with the passive attacker who uses a receiver to intrude on a WLAN.

Wireless replacement segments for wired networks are recommended where user mobility is desired. System administrators have many technology options from which to choose. With a solid knowledge of available technologies and topologies, suitable vendors can be chosen to provide the right equipment to meet the WLAN needs for any organization. Current standards offer guidance that show how wireless technologies operate, but do not relate to quality LAN design.

The analysis provided in this paper is one approach to quantifying technology and product advantages. These metrics are universal in their application and can be tailored to measure the strengths and weaknesses of various wireless networking components. With proper planning and sensible decisions, a WLAN administrator can successfully introduce wireless technology to a LAN while maintaining its previous level of security.

APPENDIX A. ABBREVIATIONS

AP - Access Point
ATM - Asynchronous Transfer Mode
BER - Bit Error Rate
bps - bits per second
BSS - Basic Service Set; A set of stations communication wirelessly on the same channel in the same area. (in IEEE 802.11)
CA - Certificate Authority
CAC - Channel Access Control (in HIPERLAN)
CAM - Channel Access Mechanism (in HIPERLAN)
ESS - Extended Service Set; A set of BSSs and wired LANs with Access Points that appear as a single logical BSS. (in IEEE 802.11)
ETR - ETSI Technical Report
ETSI - European Telecommunications Standards Institute
GSM - Global System for Mobile communications
HIPERLAN - High Performance Radio Local Area Network
HM-entity - HIPERLAN MAC entity
ICV - Integrity Check Vector
IEEE - Institute of Electrical and Electronics Engineers
ISO - International Standard Organization
IV - Initialization Vector
LAN - Local Area Network
MAC - Medium Access Control
MPDU - MAC Protocol Data Unit
PEM - Privacy Enhanced Mail
PHY - Physical layer
PRNG - Pseudo Random Number Generator
SKCS - Shared Key Cryptography System
UMTS - Universal Mobile Telecommunications System
WEP - Wired Equivalent Privacy

APPENDIX B. DEFINITIONS

Ad-hoc: In ad-hoc configuration the wireless LAN has no fixed components

Authentication: The identification of the parties base Usually fixed base station of the wireless LAN, sometimes referred as Access Point

Cipher text: The data after ciphering confidentiality Only intended parties can access the data

Coverage: The area where the transmission of the node can be heard

Denial of service: An attack preventing the system from being used

Eavesdropping: Capturing the data by an unintended party

End-to-end: From the sending node to the intended receiver

Integrity: The message can not be modified or replaced by unintended parties

Key management: The policy to distribute and save the private and public keys

Plain text: The data to be send before ciphered

Pre-arranged: In pre-arranged configuration the wireless LAN has some fixed components, like bases

Private key: A sensitive key that must not be compromised

Public key: A non-sensitive that can be published

Shared key: A secret key common to many users or network nodes

Station-to-station: From one node to the next one in the network

Transitive trust: An attack exploiting the host-host or network-network trust

APPENDIX C. OSI MODEL LAYERS

OSI Layer	Function Provided
Application	Network applications such as file transfer and terminal emulation
Presentation	Data formatting and encryption
Session	Establishment and maintenance of sessions
Transport	Provision for end-to-end reliable and unreliable delivery
Network	Delivery of packets of information, which includes routing
Data Link	Transfer of units of information, framing, and error checking
Physical	Transmission of binary data of a medium

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center..... 2
8725 John J. Kingman Road, Ste 0944
Fort Belvoir, VA 22060-6218

2. Dudley Knox Library..... 2
Naval Postgraduate School
411 Dyer Road
Monterey, CA 93943-5101

3. Chairman, Code CS 1
Computer Science Department
Naval Postgraduate School
Monterey, CA 93943-5000

4. Dr. Cynthia E. Irvine..... 2
Computer Science Department, Code CS/Ic
Naval Postgraduate School
Monterey, CA 93943

5. Professor Douglas Brinkley 1
Systems Management Department, Code SM/Bi
Naval Postgraduate School
Monterey, CA 93943

6. Joseph O'Kane..... 1
National Security Agency
Research and Development Building
R23
9800 Savage Road
Fort Meade, MD 20755-6000

7. CAPT Dan Galik..... 1
Space and Naval Warfare Systems Command
PMW 161
Building OT-1, Room 1024
4301 Pacific Highway
San Diego, CA 92110-3127

8. Commander, Naval Security Group Command..... 1
Naval Security Group Headquarters
9800 Savage Road
Suite 6585
Fort Meade, MD 20755-6585
ATTN: Mr. James Shearer

9. Mr. George Bieber 1
Defense Information Systems Agency
Center for Information Systems Security
5113 Leesburg Pike, Suite 400
Falls Church, VA 22041-3230
10. CDR Chris Perry 1
N643
Presidential Tower 1
2511 South Jefferson Davis Highway
Arlington, VA 22202
11. LT James D. Fowler 1
3908 Las Brisas
Plano, TX 75074
12. Mr. John Mildner 1
Director of Technical Operations, Code 72A
SPAWAR Systems Center, Charleston
PO Box 190022
North Charleston, SC 29419